COMPUTER FORENSICS

Computer Crime Scene Investigation

SECOND EDITION

- Comprehensive overview of the subject from information security issues to auditing methods to terrorist cyber-attacks
- Includes *Evidence Identification* and *Checklist forms*, hands-on projects, exercises, and case studies for each chapter
- CD includes tools, presentations, and demos of the latest computer forensics software

Networking

JOHN R. VACCA

Computer Forensics

Second Edition

LIMITED WARRANTY AND DISCLAIMER OF LIABILITY

THE CD-ROM THAT ACCOMPANIES THE BOOK MAY BE USED ON A SINGLE PC ONLY. THE LICENSE DOES NOT PERMIT THE USE ON A NETWORK (OF ANY KIND). YOU FURTHER AGREE THAT THIS LICENSE GRANTS PERMISSION TO USE THE PRODUCTS CONTAINED HEREIN, BUT DOES NOT GIVE YOU RIGHT OF OWNERSHIP TO ANY OF THE CONTENT OR PRODUCT CONTAINED ON THIS CD-ROM. USE OF THIRD-PARTY SOFTWARE CONTAINED ON THIS CD-ROM IS LIMITED TO AND SUBJECT TO LICENSING TERMS FOR THE RESPECTIVE PRODUCTS.

CHARLES RIVER MEDIA, INC. ("CRM") AND/OR ANYONE WHO HAS BEEN INVOLVED IN THE WRITING, CREATION, OR PRODUCTION OF THE ACCOMPANYING CODE ("THE SOFTWARE") OR THE THIRD-PARTY PRODUCTS CONTAINED ON THE CD-ROM OR TEXTUAL MATERIAL IN THE BOOK, CANNOT AND DO NOT WARRANT THE PERFORMANCE OR RESULTS THAT MAY BE OBTAINED BY USING THE SOFTWARE OR CONTENTS OF THE BOOK. THE AUTHOR AND PUBLISHER HAVE USED THEIR BEST EFFORTS TO ENSURE THE ACCURACY AND FUNCTIONALITY OF THE TEXTUAL MATERIAL AND PROGRAMS CONTAINED HEREIN. WE HOWEVER, MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE PERFORMANCE OF THESE PROGRAMS OR CONTENTS. THE SOFTWARE IS SOLD "AS IS" WITHOUT WARRANTY (EXCEPT FOR DEFECTIVE MATERIALS USED IN MANUFACTURING THE DISK OR DUE TO FAULTY WORKMANSHIP).

THE AUTHOR, THE PUBLISHER, DEVELOPERS OF THIRD-PARTY SOFTWARE, AND ANYONE INVOLVED IN THE PRODUCTION AND MANUFACTURING OF THIS WORK SHALL NOT BE LIABLE FOR DAMAGES OF ANY KIND ARISING OUT OF THE USE OF (OR THE INABILITY TO USE) THE PROGRAMS, SOURCE CODE, OR TEXTUAL MATERIAL CONTAINED IN THIS PUBLICATION. THIS INCLUDES, BUT IS NOT LIMITED TO, LOSS OF REVENUE OR PROFIT, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THE PRODUCT.

THE SOLE REMEDY IN THE EVENT OF A CLAIM OF ANY KIND IS EXPRESSLY LIMITED TO REPLACEMENT OF THE BOOK AND/OR CD-ROM, AND ONLY AT THE DISCRETION OF CRM.

THE USE OF "IMPLIED WARRANTY" AND CERTAIN "EXCLUSIONS" VARIES FROM STATE TO STATE, AND MAY NOT APPLY TO THE PURCHASER OF THIS PRODUCT.

Computer Forensics:

Computer Crime Scene Investigation

Second Edition

John R. Vacca

CHARLES RIVER MEDIA, INC.
Boston, Massachusetts

Cover Design: Tyler Creative

CHARLES RIVER MEDIA
25 Thomson Place
Boston, Massachusetts 02210
617-757-7900
617-757-7969 (FAX)
crm.info@thomson.com
www.charlesriver.com

This book is printed on acid-free paper.

John R. Vacca. *Computer Forensics: Computer Crime Scene Investigation, Second Edition.*
ISBN: 1-58450-389-0
ISBN-13: 978-1-58450-389-7
eISBN: 1-58450-637-7

Library of Congress Cataloging-in-Publication Data
Vacca, John R.
Computer forensics : computer crime scene investigation / John R. Vacca.-- 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 1-58450-389-0 (pbk. with cd-rom : alk. paper)
1. Computer security. 2. Computer networks--Security measures. 3. Forensic sciences. I. Title.
QA76.9.A25V33 2005
005.8--dc22
2005007521

Printed in the United States of America
07 7 6 5 4 3

CHARLES RIVER MEDIA titles are available for site license or bulk purchase by institutions, user groups, corporations, etc. For additional information, please contact the Special Sales Department at 800-347-7707.

Requests for replacement of a defective CD-ROM must be accompanied by the original disc, your mailing address, telephone number, date of purchase and purchase price. Please state the nature of the problem, and send the information to CHARLES RIVER MEDIA, 25 Thomson Place, Boston, Massachusetts 02210. CRM's sole obligation to the purchaser is to replace the disc, based on defective materials or faulty workmanship, but not on the operation or functionality of the product.

In memory of Giacchi and Agrippina.

This page intentionally left blank

Contents

Acknowledgments

There are many people whose efforts on this book have contributed to its successful completion. I owe each a debt of gratitude and want to take this opportunity to offer my sincere thanks.

A very special thanks to my publisher, David Pallai, without whose initial interest and support this book would not have been possible, for his guidance and encouragement over and above the business of being a publisher. Thanks also to Bryan Davidson, Ania Wieckowski, and Jennifer Blaney of Charles River Media, whose many talents and skills are essential to a finished book. Thanks to my copyeditor, Ruth Saavedra, whose fine editorial work has been invaluable. Thanks also to my marketing manager, Meg Dunkerley, whose efforts on this book have been greatly appreciated. Finally, a special thanks to Michael Erbschloe, who wrote the Foreword for this book.

Thanks to my wife, Bee Vacca, for her love, her help, and her understanding of my long work hours.

Finally, I wish to thank the organizations and individuals who granted me permission to use the research material and information necessary for the completion of this book.

This page intentionally left blank

Foreword

Computer crime and computer-supported criminal activities are booming businesses. Criminals, fraudsters, and terrorists seem to strike whenever there is an opportunity. In January of 2005 the FBI alerted the public to a variety of scams being facilitated online involving the solicitation of additional relief funds for the victims of the recent tsunami disaster. The FBI, through the Internet Crime Complaint Center (IC3), had received reports of Web sites being established purportedly to assist with collection and relief efforts. Complaints identified several schemes that involved both unsolicited incoming emails (SPAM), as well as reports of responses to posted email addresses, to assist for a fee in locating loved ones who may have been victims of the disaster. A fraudulent relief donation Web site has also been detected containing an embedded Trojan exploit which can infect the user's computer with a virus if accessed.

There have been several major inter-agency computer crime investigations conducted during the last several years including WEB-SNARE, which, on August 26, 2004, was characterized by the Attorney General as the most successful cyber crime initiative to date. In WEB-SNARE, more than 150 investigations were successfully advanced, in which more than 150,000 victims lost more than $215 million. This initiative included 150 subjects who were charged, and the execution of 170 search and/or seizure warrants. Many of the investigations included in WEB-SNARE could potentially be characterized as Identity Theft, or related to Identity Theft.

Prior to WEB-SNARE, the IC3 coordinated the development and execution of Operations E-Con and Cyber Sweep with our law enforcement and industry partners. In those initiatives, more than 200 investigations were coordinated among the various law enforcement agencies, resulting in arrests and/or charges of more than 250 individuals for engaging in a variety of cyber crimes including Identity Theft.

The FBI has also observed a continuing increase in both volume and potential impact of cyber crime with significant international elements. Identifying such trends, as well as formulating an aggressive and proactive counter-attack strategy, remains a fundamental objective of the FBI's Cyber Division. In a growing number of cases, Eastern European subjects solicit victims though job postings, email solicitations, and chat-rooms to provide detailed personal information. Once that information is obtained, they use their identities to post auctions on well-known auction sites. Funds obtained through the auction are transferred through several shell accounts, both in the U.S and abroad, and the items sold are never delivered.

In one FBI investigation initiated in 1999, the computer network of a now defunct software e-commerce company was compromised, and credit card information for approximately eight million accounts was obtained by the hackers. The compromised e-commerce company was contacted via email by the hackers who demanded money to keep them from publicly posting the obtained information on the Internet. The FBI became aware of this crime when numerous field offices received complaints from citizens who were all incorrectly charged for similar small amounts on their credit card statements. Through investigative efforts, these complaints were all linked to the hacking of the e-commerce company's system. This case has expanded into a major FBI initiative in which field offices across the country have opened approximately 50 spin-off investigations in the network compromise and extortion of over 100 United States banks and e-commerce providers by Eastern European hacking groups.

Computer crimes are impacting society in numerous ways and there is a lot of work for the good guys. Computer forensics is one of the largest growth professions of the twenty-first century. The soaring increase in the number of Internet users combined with the constant computerization of business processes has created new opportunities for computer criminals and terrorists. Study after study has consistently revealed that cyber attacks, hacking, and computer-based criminal activities are costing businesses and government organizations billions of dollars each year.

We need to train at least 100,000 more computer crime fighters in order to stem the global tide of computer attacks. Many computer professionals have asked me how they can get started in security and crime-fighting careers. My response has constantly been learn, study, train, and move forward. *Computer Forensics*, by John Vacca, is an excellent place to start establishing the required knowledge base to move into this fascinating new career field.

Computer Forensics is an excellent book for trained law enforcement personnel who desire to learn more about investigating and fighting computer crimes. *Computer Forensics* is also an excellent book for computer professionals who want to move into the rapidly growing security field and who are considering shifting their career focus to law enforcement and criminal investigation.

It is also important that computer security personnel expand their understanding of forensic processes and keep their understanding of investigative and prevention procedures up to date. Computer Forensics is an excellent book for all levels of computer security personnel to further their professional development.

John Vacca had made an excellent contribution to the computer forensics field. I highly recommend *Computer Forensics* and congratulate John Vacca on a job extremely well done.

Michael Erbschloe
Security Consultant and Author
St. Louis, Missouri

This page intentionally left blank

Introduction

Cyber criminals are wreaking havoc on computer systems and are capturing front-page headlines in the bargain. It has made little difference that the Bush administration pledged billions in additional federal funding to combat security breaches after the 9-11 terrorists attacks. The problem just keeps getting worse.

Fortunately, the computer security field is also progressing at a brisk rate. In particular, the field of computer forensics brings new ways of preserving and analyzing evidence related to cyber crime.

GROWING PROBLEM

The numbers are chilling. According to a recent industry survey, 94% of the survey respondents detected cyberattacks on their companies, and 617 organizations reported $609,923,384 in financial losses.

So what's going on? It doesn't take a computer engineer or computer scientist to learn hacking fundamentals. After spending a few nights on the Internet, high school students discover they can master hacking fundamentals by simply downloading software. Corporations and the federal government are just beginning to realize that securing their computer networks is critical. Equally frightening is that our national security has already been compromised. Colleges have finally started to offer courses and concentrations in computer security and forensics, but it remains difficult to find degree programs in these disciplines.

COMPUTER FORENSICS

Computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored as data or magnetically encoded information.

The fascinating part of the science is that the computer evidence is often transparently created by the computer's operating system without the knowledge of the computer operator. The information may actually be hidden from view. To find it, special forensic software tools and techniques are required.

Emerging Field–But a Shortage of Experts

Most law enforcement agencies, especially those in large cities, are understaffed when it comes to having trained computer forensics experts. Industry, on the other hand, has been taking computer forensics seriously for several years. Sadly, it took a number of embarrassing computer break-ins by teenage hackers to put the spotlight on it. The problem is, industry doesn't know which computer forensics issues to focus on.

The biggest issue surrounding the computer forensics conundrum is a shortage of technologists who have a working knowledge of computer forensics. Academics are teaching the subjects, but most lack real-world experience, which is critical when training students. Also, many academics are not current with forensics trends and tools.

Times Are Changing

There's an old saying, "If you wait long enough, it's bound to change." The same can be said for computer forensics training. Not only will more techies be concentrating on computer forensics, but also attorneys and judges will be taking courses in the subject. Learning forensics basics will help attorneys especially to determine the kinds of evidence that can be found by probing a computer's operating system and what techniques can be used to legally obtain it.

On the academic front, full-fledged degree tracks in computer forensics are being developed. Certification programs already exist.

Where are the jobs? Government agencies, such as the Department of Defense, FBI, CIA, NSA, and U.S. Postal Service need computer forensics specialists. State and local law enforcement departments are also hiring computer forensics specialists. On the corporate front, all companies (especially large and mid-size ones with a Web presence) will have serious computer forensics needs. Job titles differ, but, typically, these positions are advertised as junior computer forensics analysts for entry-level jobs and senior computer forensics analysts if you have a few years of experience in the field.

PURPOSE

The purpose of this book is to show experienced (intermediate to advanced) computer forensics, security, and law enforcement professionals how to analyze and conduct a computer forensics examination and report the findings that will lead to the incarceration of the perpetrators. This book also provides the fundamental knowledge you need to analyze risks to your system and implement a workable security and forensics policy that protects your information assets from potential intrusion, damage, or theft. Through extensive hands-on examples (field and trial experiments) and case studies, you will gain the knowledge and skills required to master the deployment of information warfare countermeasures to thwart potential attacks.

SCOPE

Throughout the book, extensive hands-on examples presented at the end of each chapter in the form of exercises, case studies, projects, and checklists (located in Appendix F), will provide you with practical experience in computer forensics evidence capture, analysis, and reporting, as well as information warfare countermeasures and future directions. In addition to advanced computer forensics technology considerations in commercial organizations and governments, the book addresses, but is not limited to, the following line items as part of the discovery of electronic evidence:

ON THE CD

- The CD-ROM that accompanies this book contains the latest and best computer forensics software tools and documentation.
- You will learn how to analyze your exposure to security threats and protect your organization's systems and data; manage risks emanating from inside the organization and from the Internet and extranets; protect network users from hostile applications and viruses; reduce your susceptibility to an attack by deploying firewalls, data encryption, decryption, and other information warfare countermeasures; and identify the security risks that need to be addressed in security and computer forensics policy.
- Chapters on how to gain practical experience in analyzing the security risks and information warfare countermeasures that need to be addressed in your organization also include maintaining strong authentication and authenticity, preventing eavesdropping, retaining integrity of information, evaluating the strength of user passwords, selecting a firewall topology, and evaluating computer and hacker ethics.

This book leaves little doubt that the new and emerging field of computer forensics is about to evolve. This new area of knowledge is now being researched, organized, and taught. No question, this book will benefit organizations and governments, as well as their computer forensics and security professionals.

TARGET AUDIENCE

With regard to computer forensics, the book is primarily targeted at those in government and law enforcement who require the fundamental skills to develop and implement security schemes designed to protect their organizations' information from attacks, including managers, network and systems administrators, technical staff, and support personnel. This also includes those involved in securing Web sites, including Web developers, Webmasters, and systems, network, and security administrators.

ORGANIZATION OF THIS BOOK

This book is organized into six parts, including the appendixes (which include a glossary of computer forensic and information warfare terms).

Part I: Overview of Computer Forensics Technology

Part I discusses computer forensics fundamentals, types of computer forensics technology, types of computer forensics systems, and vendor and computer forensics services.

Chapter 1, Computer Forensics Fundamentals, provides an overview of computer forensics types and techniques and their electronic evidence and capture.

Chapter 2, Types of Computer Forensics Technology, covers the basic issues dealing with Windows NT, Windows XP, and 2003, and their use within law enforcement computer forensic technology. In other words, it covers security and computer evidence issues associated with Windows NT, Windows XP, and 2003.

Chapter 3, Types of Computer Forensics Systems, covers different types of computer forensics systems and identifies crucial questions for corporate planning in support of computer forensics. Answering the questions raised in this chapter will assist managers in creating sound corporate security policies and practices that support the following computer forensics systems: Internet security, intrusion detection, firewall security, storage area networks security, network disaster recovery, public key infrastructure security, wireless network security, satellite encryption security, instant messaging (IM) security, Net privacy, ID management security, ID theft prevention, biometric security, and homeland security.

Chapter 4, Vendor and Computer Forensics Services, covers how a swift and measured forensic incident response—drawing on sound policies, vendor tools, and support—allows an organization to contain the potential damage of an attack and effectively seek compensation or prosecution. In addition, this chapter covers the following computer forensic services: forensic incident response, evidence collection, forensic analysis, expert witness, forensic litigation and insurance claims support, training, and forensic process improvement.

Part II: Computer Forensics Evidence and Capture

The second part of this book discusses data recovery, evidence collection and data seizure, duplication and preservation of digital evidence, and computer image verification and authentication.

Chapter 5, Data Recovery, answers many questions about the ins and outs of data recovery as it relates to computer forensics.

Chapter 6, Evidence Collection and Data Seizure, points out the difficulties in collecting evidence and seizing data and what must be done to overcome them. Not everything is covered here—it should be used as a guide only, and you should seek further information for your specific circumstances.

Chapter 7, Duplication and Preservation of Digital Evidence, is a discussion of how to keep Murphy's law from ruining your case. When it comes to computer evidence processing, Murphy is always looking over your shoulder. He stands ready to strike at just the wrong moment.

Chapter 8, Computer Image Verification and Authentication, discusses the overall security of a computer image verification and authentication system and how it rests with the combination of security measures.

Part III: Computer Forensics Analysis

Part III covers the discovery of electronic evidence, identification of data, reconstructing past events, and networks.

Chapter 9, Discovery of Electronic Evidence, addresses the process of information discovery. The fact that information discovery only deals with logical evidence (electronic data) means you can avoid much of the tedium required by search and seizure to ensure evidence integrity and the chain of custody.

Chapter 10, Identification of Data, specifically focuses on the long-recognized value of deterrence—through threat of retaliation—as an effective means of defense. The means for enabling deterrence in the cyberrealm will be introduced here.

Chapter 11, Reconstructing Past Events, illustrates the reconstruction of past events with as little distortion or bias as possible.

Chapter 12, Networks, introduces a solution to the dilemma of network forensics. Network forensics is the principle of reconstructing the activities leading up to an event and determining the answer to "What did they do?" and "How did they do it?"

Part IV: Countermeasures: Information Warfare

Part IV discusses how to fight against macro threats (defensive strategies for governments and industry groups), the information warfare arsenal and tactics of the military, the information warfare arsenal and tactics of terrorists and rogues, the information warfare arsenal and tactics of private companies, the information warfare arsenal of the future, surveillance tools for information warfare of the future, and civilian causalities (the victims and refugees of information warfare).

Chapter 13, Fighting Against Macro Threats: Defensive Strategies for Governments and Industry Groups, is an in-depth examination of the implications of information warfare for the U.S. and allied infrastructures that depend on the unimpeded management of information that is also required in the fight against macro threats (defensive strategies for governments and industry groups).

Chapter 14, The Information Warfare Arsenal and Tactics of the Military, focuses on two goals. First, you need to find a way to protect yourself against catastrophic events. Second, you need to build a firm foundation on which you can make steady progress by continually raising the cost of mounting an attack and mitigating the expected damage of the information warfare arsenal and tactics of the military.

Chapter 15, The Information Warfare Arsenal and Tactics of Terrorists and Rogues, recommends a number of specific steps that could better prepare the U.S. military and private companies to confront "the new terrorism" and its information warfare arsenal and tactics.

Chapter 16, The Information Warfare Arsenal and Tactics of Private Companies, deals with the information warfare tools and strategies of private companies and how they're used against the aggressors. It will also help to realistically guide the process of moving forward in dealing with the information warfare arsenal and tactics of private companies.

Chapter 17, The Information Warfare Arsenal of the Future, discusses how the increasing dependence on sophisticated information systems brings with it an increased vulnerability to hostile elements, terrorists among them, in dealing with the information warfare arsenal of the future.

Chapter 18, Surveillance Tools for Information Warfare of the Future, discusses the basic concepts and principles that must be understood and that can help guide the process of moving forward in dealing with the surveillance tools for the information warfare of the future.

Chapter 19, Civilian Casualities: The Victims and Refugees of Information Warfare, considers the application of civilian information operations (CIOs) to the conventional warfare environment. Although the array of CIO tools and techniques has been presented as discrete elements in a schematic diagram, the CIO environment is complex, multidimensional, interactive, and still developing.

Part V: Advanced Computer Forensics Systems and Future Directions

Finally, Part V discusses advanced computer forensics, with a summary, conclusions, and recommendations.

Chapter 20, Advanced Computer Forensics, introduces numerous solutions for those of you who are in the process of conducting advanced computer forensics through the use of encryption for protection and hacking back with advanced hacker trackers.

Chapter 21, Summary, Conclusions, and Recommendations. No summary chapter on computer forensics would be complete without an examination of costs involved. This final chapter is concerned with how to conduct a relevant and meaningful review of computer forensic analysis software tools. It is also the intent of this chapter to initiate discussions to solidify the various computer forensics requirements. Finally, this chapter recommends the establishment of computer forensics standards for the exchange of digital evidence between sovereign nations and is intended to elicit constructive discussions regarding digital evidence.

Appendixes

Eight appendixes provide additional resources that are available for computer forensics. Appendix A is a list of frequently asked questions. Appendix B is a list of computer forensic resources. Appendix C contains links to computer forensics and related law enforcement Web pages. Appendix D contains more computer forensics case studies. Appendix E contains answers to review questions and exercises, hands-on projects, case projects, and optional team case projects by chapter. Appendix F contains checklists by chapter. Appendix G contains all of the files that are on the CD-ROM. The book ends with Appendix H—a glossary of computer forensics and information-warfare-related terms.

CONVENTIONS

This book uses several conventions to help you find your way around and to help you find important sidebars, facts, tips, notes, cautions, and warnings. You see eye-catching icons in the left margin from time to time. They alert you to critical information and warn you about problems.

John R. Vacca
jvacca@hti.net

Part I

Overview of Computer Forensics Technology

Part One discusses computer forensics fundamentals, types of computer forensics technology, types of computer forensics systems, and vendor and computer forensics services.

This page intentionally left blank

1 Computer Forensics Fundamentals

Electronic evidence and information gathering have become central issues in an increasing number of conflicts and crimes. Electronic or computer evidence used to mean the regular print-out from a computer—and a great deal of computer exhibits in court are just that. However, for many years, law enforcement officers have been seizing data media and computers themselves, as they have become smaller and more ubiquitous.

In the very recent past, investigators generated their own printouts, sometimes using the original application program, sometimes specialist analytic and examination tools. More recently, investigators have found ways of collecting evidence from remote computers to which they do not have immediate physical access, provided such computers are accessible via a phone line or network connection. It is even possible to track activities across a computer network, including the Internet.

These procedures form part of what is called *computer forensics,* though some people also use the term to include the use of computers to analyze complex data (for example, connections between individuals by examination of telephone logs or bank account transactions). Another use of the term is when computers are employed in the court itself, in the form of computer graphics, to illustrate a complex situation such as a fraud or as a replacement for large volumes of paper-based exhibits and statements.

So, what actually is computer forensics? Computer forensics is about evidence from computers that is sufficiently reliable to stand up in court and be convincing. You might employ a computer forensics specialist to acquire evidence from computers on your behalf. On the other hand, you may want one to criticize the work of others. The field is a rapidly growing one, with a solid core but with many controversies at its edges.

INTRODUCTION TO COMPUTER FORENSICS

Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user.

In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence. Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings.

Far more information is retained on a computer than most people realize. It's also more difficult to completely remove information than is generally thought. For these reasons (and many more), computer forensics can often find evidence of, or even completely recover, lost or deleted information, even if the information was intentionally deleted.

Computer forensics, although employing some of the same skills and software as data recovery, is a much more complex undertaking. In data recovery, the goal is to retrieve the lost data. In computer forensics, the goal is to retrieve the data and interpret as much information about it as possible.

The continuing technological revolution in communications and information exchange has created an entirely new form of crime: cyber crime or computer crime. Computer crime has forced the computer and law enforcement professions to develop new areas of expertise and avenues of collecting and analyzing evidence. This is what has developed into the science of computer forensics. The process of acquiring, examining, and applying digital evidence is crucial to the success of prosecuting a cyber criminal. With the continuous evolution of technology, it is difficult for law enforcement and computer professionals to stay one step ahead of technologically savvy criminals. To effectively combat cyber crime, greater emphasis must be placed in the computer forensic field of study, including but not limited to financial support, international guidelines and laws, and training of the professionals involved in the process, as well as the following subject matter:

- Computer crime
- The computer forensic objective
- The computer forensic priority
- The accuracy versus speed conflict
- The need for computer forensics
- The double tier approach

- Requirements for the double tier approach
- The computer forensics specialist

Computer Crime

According to industry analysts, there are currently 657 million people online worldwide. That figure is expected to rise to 794 million by 2009. This represents a lot of data interchange. Unfortunately many small businesses, and even large organizations, do not know how to properly protect their sensitive data, thus leaving the door open to criminals.

Computers can be involved in a wide variety of crimes including white-collar crimes, violent crimes such as murder and terrorism, counterintelligence, economic espionage, counterfeiting, and drug dealing. A 2003 FBI survey reported that the average bank robbery netted $6,900, whereas the average computer crime netted $900,000 [1]. The Internet has made targets much more accessible, and the risks involved for the criminal are much lower than with traditional crimes. A person can sit in the comfort of his home or a remote site and hack into a bank and transfer millions of dollars to a fictitious account, in essence robbing the bank, without the threat of being gunned down while escaping. One hears of such technological crimes almost daily, thus creating a perception of lawlessness in the cyber world. The same FBI survey revealed that both public and private agencies face serious threats from external as well as internal sources. Out of the 849 organizations that responded to the survey, 30% claimed theft of proprietary information, 23% reported sabotage of data or their networks, 35% experienced system penetration from an outside source, and 12% claimed financial fraud. More alarming is the ease of access to sensitive data employees have within the organization. Fifty-nine percent of the organizations involved in the survey reported employees having unauthorized access to corporate information.

Recently a survey was conducted to determine where the FBI was focusing their computer forensic efforts. An alarming 74% of their workload is centered on white-collar crime. This type of crime includes health care fraud, government fraud including erroneous IRS and Social Security benefit payments, and financial institution fraud. These are high-dollar crimes made easy by technology. The other 26% of the workload is split equally among violent crime (child pornography, interstate theft), organized crime (drug dealing, criminal enterprise), and counterterrorism and national security. As shown by this survey, computer crime is widespread and has infiltrated areas unimaginable just a few years ago. The FBI caseload has gone from near zero in 1985 to nearly 10,000 cases in 2003. It is no doubt considerably higher today. They have gone from two part-time scientists to

899 personnel in regional field offices throughout the country. Technology has brought this field of study to the forefront.

Roles of a Computer in a Crime

A computer can play one of three roles in a computer crime. A computer can be the target of the crime, it can be the instrument of the crime, or it can serve as an evidence repository storing valuable information about the crime. In some cases, the computer can have multiple roles. It can be the "smoking gun" serving as the instrument of the crime. It can also serve as a file cabinet storing critical evidence. For example, a hacker may use the computer as the tool to break into another computer and steal files, then store them on the computer. When investigating a case, it is important to know what roles the computer played in the crime and then tailor the investigative process to that particular role.

Applying information about how the computer was used in the crime also helps when searching the system for evidence. If the computer was used to hack into a network password file, the investigator will know to look for password cracking software and password files. If the computer was the target of the crime, such as an intrusion, audit logs and unfamiliar programs should be checked. Knowing how the computer was used will help narrow down the evidence collection process. With the size of hard drives these days, it can take a very long time to check and analyze every piece of data a computer contains. Often law enforcement officials need the information quickly, and having a general idea of what to look for will speed the evidence collection process.

The Computer Forensic Objective

The objective in computer forensics is quite straightforward. It is to recover, analyze, and present computer-based material in such a way that it is useable as evidence in a court of law. The key phrase here is *useable as evidence in a court of law*. It is essential that none of the equipment or procedures used during the examination of the computer obviate this.

The Computer Forensic Priority

Computer forensics is concerned primarily with forensic procedures, rules of evidence, and legal processes. It is only secondarily concerned with computers. Therefore, in contrast to all other areas of computing, where speed is the main concern, in computer forensics the absolute priority is accuracy. One talks of completing work as efficiently as possible, that is, as fast as possible without sacrificing accuracy.

Accuracy Versus Speed

In this seemingly frenetic world where the precious resource of time is usually at a premium, pressure is heaped upon you to work as fast as possible. Working under such pressure to achieve deadlines may induce people to take shortcuts in order to save time.

In computer forensics, as in any branch of forensic science, the emphasis must be on evidential integrity and security. In observing this priority, every forensic practitioner must adhere to stringent guidelines. Such guidelines do not encompass the taking of shortcuts, and the forensic practitioner accepts that the precious resource of time must be expended in order to maintain the highest standards of work.

The Computer Forensics Specialist

A computer forensics specialist is the person responsible for doing computer forensics. The computer forensics specialist will take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject computer system:

1. Protect the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.
2. Discover all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
3. Recover all (or as much as possible) of discovered deleted files.
4. Reveal (to the extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.
5. Accesses (if possible and if legally appropriate) the contents of protected or encrypted files.
6. Analyze all possibly relevant data found in special (and typically inaccessible) areas of a disk. This includes but is not limited to what is called unallocated space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as slack space in a file (the remnant area at the end of a file, in the last assigned disk cluster, that is unused by current file data but once again may be a possible site for previously created and relevant evidence).
7. Print out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data. Further, provide an opinion of the system layout; the file structures discovered; any discovered data and authorship information; any attempts to hide, delete, protect, or encrypt information; and anything else that has been discovered and appears to be relevant to the overall computer system examination.
8. Provide expert consultation and/or testimony, as required [2].

Who Can Use Computer Forensic Evidence?

Many types of criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialists.

- Criminal Prosecutors use computer evidence in a variety of crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.
- Civil litigations can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases. Insurance companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.
- Corporations often hire computer forensics specialists to find evidence relating to sexual harassment, embezzlement, theft or misappropriation of trade secrets, and other internal/confidential information.
- Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment. The use of computer forensics in law enforcement is discussed in detail in the next section and throughout the book.
- Individuals sometimes hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment, or age discrimination [2].

USE OF COMPUTER FORENSICS IN LAW ENFORCEMENT

If there is a computer on the premises of a crime scene, the chances are very good that there is valuable evidence on that computer. If the computer and its contents are examined (even if very briefly) by anyone other than a trained and experienced computer forensics specialist, the usefulness and credibility of that evidence will be tainted.

Choosing a Computer Forensics Specialist for a Criminal Case

When you require the services of a computer forensics specialist, don't be afraid to shop around. There are an increasing number of people who claim to be experts in the field. Look very carefully at the level of experience of the individuals involved. There is far more to proper computer forensic analysis than the ability to retrieve data, especially when a criminal case is involved. Think about computer forensics just as you would any other forensic science and look for a corresponding level of expertise.

The bottom line is that you will be retaining the services of an individual who will likely be called to testify in court to explain what he or she did to the computer and its data. The court will want to know that individual's own level of training and experience, not the experience of his or her employer. Make sure you find someone who not only has the expertise and experience, but also the ability to stand up to the scrutiny and pressure of cross-examination.

COMPUTER FORENSICS ASSISTANCE TO HUMAN RESOURCES/EMPLOYMENT PROCEEDINGS

Computer forensics analysis is becoming increasingly useful to businesses. Computers can contain evidence in many types of human resources proceedings, including sexual harassment suits, allegations of discrimination, and wrongful termination claims. Evidence can be found in electronic mail systems, on network servers, and on individual employee's computers. However, due to the ease with which computer data can be manipulated, if the search and analysis is not performed by a trained computer forensics specialist, it could likely be thrown out of court.

Employer Safeguard Program

As computers become more prevalent in businesses, employers must safeguard critical business information. An unfortunate concern today is the possibility that data could be damaged, destroyed, or misappropriated by a discontented individual.

Before an individual is informed of their termination, a computer forensic specialist should come on-site and create an exact duplicate of the data on the individual's computer. In this way, should the employee choose to do anything to that data before leaving, the employer is protected. Damaged or deleted data can be replaced, and evidence can be recovered to show what occurred. This method can also be used to bolster an employer's case by showing the removal of proprietary information or to protect the employer from false charges made by the employee.

Whether you are looking for evidence in a criminal prosecution or civil suit or determining exactly what an employee has been up to, you should be equipped to find and interpret the clues that have been left behind. This includes situations where files have been deleted, disks have been reformatted, or other steps have been taken to conceal or destroy the evidence. For example, did you know

- What Web sites have been visited
- What files have been downloaded
- When files were last accessed
- Of attempts to conceal or destroy evidence
- Of attempts to fabricate evidence

- That the electronic copy of a document can contain text that was removed from the final printed version
- That some fax machines can contain exact duplicates of the last several hundred pages received
- That faxes sent or received via computer may remain on the computer indefinitely
- That email is rapidly becoming the communications medium of choice for businesses
- That people tend to write things in email that they would never consider writing in a memorandum or letter
- That email has been used successfully in criminal cases as well as in civil litigation
- That email is often backed up on tapes that are generally kept for months or years
- That many people keep their financial records, including investments, on computers [3]

COMPUTER FORENSICS SERVICES

No matter how careful they are, when people attempt to steal electronic information (everything from customer databases to blueprints), they leave behind traces of their activities. Likewise, when people try to destroy incriminating evidence contained on a computer (from harassing memos to stolen technology), they leave behind vital clues. In both cases, those traces can prove to be the smoking gun that successfully wins a court case. Thus, computer data evidence is quickly becoming a reliable and essential form of evidence that should not be overlooked.

A computer forensics professional does more than turn on a computer, make a directory listing, and search through files. Your forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case. For example, they should be able to perform the following services:

- Data seizure
- Data duplication and preservation
- Data recovery
- Document searches
- Media conversion
- Expert witness services
- Computer evidence service options
- Other miscellaneous services

Data Seizure

Federal rules of civil procedure let a party or their representative inspect and copy designated documents or data compilations that may contain evidence. Your computer forensics experts, following federal guidelines, should act as this representative, using their knowledge of data storage technologies to track down evidence [3]. Your experts should also be able to assist officials during the equipment seizure process. See Chapter 6, "Evidence Collection and Data Seizure," for more detailed information.

Data Duplication and Preservation

When one party must seize data from another, two concerns must be addressed: the data must not be altered in any way, and the seizure must not put an undue burden on the responding party. Your computer forensics experts should acknowledge both of these concerns by making an exact duplicate of the needed data. Because duplication is fast, the responding party can quickly resume its normal business functions, and, because your experts work on the duplicated data, the integrity of the original data is maintained. See Chapter 7, "Duplication and Preservation of Digital Evidence," for more detailed information.

Data Recovery

Using proprietary tools, your computer forensics experts should be able to safely recover and analyze otherwise inaccessible evidence. The ability to recover lost evidence is made possible by the expert's advanced understanding of storage technologies. For example, when a user deletes an email, traces of that message may still exist on the storage device. Although the message is inaccessible to the user, your experts should be able to recover it and locate relevant evidence. See Chapter 5, "Data Recovery," for more detailed information.

Document Searches

Your computer forensics experts should also be able to search over 200,000 electronic documents in seconds rather than hours. The speed and efficiency of these searches make the discovery process less complicated and less intrusive to all parties involved.

Media Conversion

Some clients need to obtain and investigate computer data stored on old and unreadable devices. Your computer forensics experts should extract the relevant data from these devices, convert it into readable formats, and place it onto new storage media for analysis.

Expert Witness Services

Computer forensics experts should be able to explain complex technical processes in an easy-to-understand fashion. This should help judges and juries comprehend how computer evidence is found, what it consists of, and how it is relevant to a specific situation (see sidebar, "Provide Expert Consultation and Expert Witness Services").

PROVIDE EXPERT CONSULTATION AND EXPERT WITNESS SERVICES

COMPUTERS

Expert Testimony

- Has testified multiple times as an expert witness in computers and computer forensics in circuit court
- Regularly testify as an expert witness in computers and computer forensics in federal court for U.S. attorney's offices

Computer Expertise

- Belongs to the Computer Crime Investigators Association
- Trained in the forensic examination of computers (PC & Mac), having conducted examinations in countless cases including child exploitation, homicide, militia, software piracy, and fraud
- Has testified in state and federal courts as an expert in computers, computer forensics, the Internet, and America Online; often as an expert witness for U.S. attorney's offices
- Is thoroughly familiar with both computer hardware and software, having written software and repaired and assembled computers
- Teaches computer crime investigation, including computer search and seizure, for the Institute of Police Technology and Management
- Regularly consults with law enforcement officers in the search and seizure of computers
- Has provided forensic training to numerous law enforcement officers and corporate security officers
- Regularly consulted by other forensic examiners for advice in difficult cases

Training Given as Expert in Computer Crimes

- Law Enforcement and Corrections Technology Symposium and Exhibition
- Bureau of Justice Statistics/Justice Research Statistics Association

→

Electronic Surveillance

- Theft by employees or others
  - Time
  - Property
  - Propriety information and trade secrets
- Embezzlement
- Inappropriate employee actions
- Burglary

Your computer forensics expert's experience should include installing cameras in every imaginable location (indoors and outdoors, offices, homes, warehouses, stores, schools, or vehicles) for every conceivable crime (theft, burglaries, homicides, gambling, narcotics, prostitution, extortion, or embezzlement) under every conceivable circumstance (controlled settings, hostage crisis, or court-ordered covert intrusion).

If you need to know what your employees are doing on your time and on your premises, your computer forensics experts should be able to covertly install video monitoring equipment so that you can protect your interests. This even includes situations where employees may be misusing company computers. By using video surveillance to document employees who are stealing time, property, or secrets from you, you should protect yourself if you plan to take appropriate action against the employees.

Child Exploitation

- Child sexual exploitation
- Child pornography
  - Manufacture
  - Use
  - Sale
  - Trading
  - Collection
  - Child erotica
- Use of computers in child exploitation
- Search and seizure
- Victim acquisition
- Behavior of preferential and situational offenders
- Investigation
  - Proactive
  - Reactive [4]

Computer Evidence Service Options

Your computer forensics experts should offer various levels of service, each designed to suit your individual investigative needs. For example, they should be able to offer the following services:

- Standard service
- On-site service
- Emergency service
- Priority service
- Weekend service

Standard Service

Your computer forensics experts should be able to work on your case during normal business hours until your critical electronic evidence is found. They must be able to provide clean rooms and ensure that all warranties on your equipment will still be valid following their services.

On-Site Service

Your computer forensics experts should be able to travel to your location to perform complete computer evidence services. While on-site, the experts should quickly be able to produce exact duplicates of the data storage media in question. Their services should then be performed on the duplicate, minimizing the disruption to business and the computer system. Your experts should also be able to help federal marshals seize computer data and be very familiar with the Federal Guidelines for Searching and Seizing Computers.

Emergency Service

After receiving the computer storage media, your computer forensics experts should be able to give your case the highest priority in their laboratories. They should be able to work on it without interruption until your evidence objectives are met.

Priority Service

Dedicated computer forensics experts should be able to work on your case during normal business hours (8:00 A.M. to 5:00 P.M., Monday through Friday) until the evidence is found. Priority service typically cuts your turnaround time in half.

Weekend Service

Computer forensics experts should be able to work from 8:00 A.M. to 5:00 P.M., Saturday and Sunday, to locate the needed electronic evidence and will continue working on your case until your evidence objectives are met. Weekend service depends on the availability of computer forensics experts.

Other Miscellaneous Services

Computer forensics experts should also be able to provide extended services. These services include

- Analysis of computers and data in criminal investigations
- On-site seizure of computer data in criminal investigations
- Analysis of computers and data in civil litigation.
- On-site seizure of computer data in civil litigation
- Analysis of company computers to determine employee activity
- Assistance in preparing electronic discovery requests
- Reporting in a comprehensive and readily understandable manner
- Court-recognized computer expert witness testimony
- Computer forensics on both PC and Mac platforms
- Fast turnaround time

Recover Data You Thought Was Lost Forever

Computers systems may crash. Files may be accidentally deleted. Disks may accidentally be reformatted. Computer viruses may corrupt files. Files may be accidentally overwritten. Disgruntled employees may try to destroy your files. All of these can lead to the loss of your critical data. You may think it's lost forever, but computer forensics experts should be able to employ the latest tools and techniques to recover your data.

In many instances, the data cannot be found using the limited software tools available to most users. The advanced tools that computer forensics experts utilize allow them to find your files and restore them for your use. In those instances where the files have been irreparably damaged, the experts' computer forensics expertise allows them to recover even the smallest remaining fragments.

Advise You on How to Keep Your Data and Information Safe from Theft or Accidental Loss

Business today relies on computers. Your sensitive client records or trade secrets are vulnerable to intentional attacks from, for example, computer hackers, disgruntled employees, viruses, and corporate espionage. Equally threatening, but far less considered, are unintentional data losses caused by accidental deletion, computer hardware and software crashes, and accidental modification.

Computer forensics experts should advise you on how to safeguard your data by such methods as encryption and back-up. The experts can also thoroughly clean sensitive data from any computer system you plan on eliminating.

Your files, records, and conversations are just as vital to protect as your data. Computer forensics experts should survey your business and provide guidance for improving the security of your information. This includes possible information leaks such as cordless telephones, cellular telephones, trash, employees, and answering machines.

Examine a Computer to Find Out What Its User Has Been Doing

Whether you're looking for evidence in a criminal prosecution, looking for evidence in a civil suit, or determining exactly what an employee has been up to, your computer forensics experts should be equipped to find and interpret the clues that have been left behind. This includes situations where files have been deleted, disks have been reformatted, or other steps have been taken to conceal or destroy evidence.

As previously mentioned, your computer forensics experts should provide complete forensic services. These include electronic discovery consultation, on-site seizure of evidence, thorough processing of evidence, interpretation of the results, reporting the results in an understandable manner, and court-recognized expert testimony.

Your computer forensics experts should also be able to regularly provide training to other forensic examiners, from both the government and private sectors. When other forensic examiners run into problems, they should turn to your experts for solutions.

Sweep Your Office for Listening Devices

In today's high-tech society, bugging devices, ranging from micro-miniature transmitters to micro-miniature recorders, are readily available. Automatic telephone-recording devices are as close as your nearest Radio Shack store. Your computer forensics experts should have the equipment and expertise to conduct thorough electronic countermeasures (ECM) sweeps of your premises.

High-Tech Investigations

Your computer forensics experts should have high level government investigative experience and the knowledge and experience to conduct investigations involving technology, whether the technology is the focus of the investigation or is required to conduct the investigation. The experts should be uniquely qualified to conduct investigations involving cellular telephone cloning, cellular subscription fraud, software piracy, data or information theft, trade secrets, computer crimes, misuse of computers by employees, or any other technology issue.

So, what are your employees actually doing? Are they endlessly surfing the Web? Are they downloading pornography and opening your company to a sexual harassment lawsuit? Are they emailing trade secrets to your competitors? Are they running their own business from your facilities while they are on your clock?

Your computer forensics experts should be uniquely qualified to answer these questions and many more. Don't trust these sensitive inquiries to companies that don't have the required expertise. *Trust no one!*

For a detailed discussion of the preceding computer forensics services, see Chapter 4, "Vendor and Computer Forensics Services." Now, let's examine how evidence might be sought in a wide range of computer crime or misuse, including theft of trade secrets, theft or destruction of intellectual property, and fraud. Computer specialists can draw on an array of methods of discovering data that resides in a computer system or for recovering deleted, encrypted, or damaged file information. Any or all of this information may help during discovery, depositions, or litigation.

BENEFITS OF PROFESSIONAL FORENSICS METHODOLOGY

The impartial computer forensics expert who helps during discovery will typically have experience on a wide range of computer hardware and software. It is always beneficial when your case involves hardware and software with which this expert is directly familiar, but fundamental computer design and software implementation is often quite similar from one system to another. Experience in one application or operating system area is often easily transferable to a new system.

Unlike paper evidence, computer evidence can often exist in many forms, with earlier versions still accessible on a computer disk. Knowing the possibility of their existence, even alternate formats of the same data can be discovered. The discovery process can be served well by a knowledgeable expert identifying more possibilities that can be requested as possibly relevant evidence. In addition, during on-site premises inspections, for cases where computer disks are not actually seized or forensically copied, the forensics expert can more quickly identify places to look, signs to look for, and additional information sources for relevant evidence. These may take the form of earlier versions of data files (memos, spreadsheets) that still exist on the computer's disk or on backup media or differently formatted versions of data, either created or treated by other application programs (word processing, spreadsheet, email, timeline, scheduling, or graphic).

Protection of evidence is critical. A knowledgeable computer forensics professional should ensure that a subject computer system is carefully handled to ensure that

- No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer

- No possible computer virus is introduced to a subject computer during the analysis process
- Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage
- A continuing chain of custody is established and maintained
- Business operations are affected for a limited amount of time, if at all
- Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged [2].

Steps Taken by Computer Forensics Specialists

The computer forensics specialist needs to complete an Evidence Identification and Retrieval Checklist (as shown in Table F1.1 in Appendix F) [2]. He or she should take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject's computer system.

WHO CAN USE COMPUTER FORENSIC EVIDENCE?

Many types of criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialists. These are as follows:

- Criminal prosecutors use computer evidence in a variety of crimes where incriminating documents can be found, including homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.
- Civil litigations can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases.
- Insurance companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.
- Corporations often hire computer forensics specialists to find evidence relating to sexual harassment, embezzlement, and theft or misappropriation of trade secrets, and other internal and confidential information.
- Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.
- Individuals sometimes hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment, or age discrimination.

However, there are concerns and problems with computer forensic evidence. Let's examine some of those problems.

Problems with Computer Forensic Evidence

Computer evidence is like any other evidence. It must be

- Authentic
- Accurate
- Complete
- Convincing to juries
- In conformity with common law and legislative rules (i.e., admissible) [5]

There are also special problems:

- Computer data changes moment by moment.
- Computer data is invisible to the human eye; it can only be viewed indirectly after appropriate procedures.
- The process of collecting computer data may change it—in significant ways. The processes of opening a file or printing it out are not always neutral.
- Computer and telecommunications technologies are always changing so that forensic processes can seldom be fixed for very long [5].

The Forensic Technician

Contrary to what is often thought, in many cases it is possible to produce reliable computer-derived evidence without recourse to specialist tools. The general principles are:

- The scene of crime has to be frozen; that is, the evidence has to be collected as early as possible and without any contamination.
- There must be continuity of evidence, sometimes known as chain of custody; that is, it must be possible to account for all that has happened to the exhibit between its original collection and its appearance in court, preferably unaltered.
- All procedures used in examination should be auditable; that is, a suitably qualified independent expert appointed by the other side in a case should be able to track all the investigations carried out by the prosecution's experts [5].

Good results can be obtained by using the standard disk repair, network testing, and other utilities; however, complete records need to be kept. Even so, for some purposes these may not be enough, for example, where it is hoped to recover previously deleted material or where a logic bomb or virus is suspected. In these circumstances, specialist tools are needed. Special training is also required. The tools themselves don't address all of the problems of producing evidence that will stand up in court. Thus, the key features of the forensic technician are

- Careful methodology of approach, including record keeping
- A sound knowledge of computing, particularly in any specialist areas claimed
- A sound knowledge of the law of evidence
- A sound knowledge of legal procedures
- Access to and skill in the use of appropriate utilities [5]

Legal Tests

The rules vary from legislation to legislation, but one can give a broad outline of what happens in those countries with a common law tradition—the U.K., U.S., and the so-called old Commonwealth. The law makes distinctions between real evidence, testimonial evidence, and hearsay. Real evidence is that which comes from an inanimate object that can be examined by the court. Testimonial evidence is that which a live witness has seen and upon which he or she can be cross-examined. The hearsay rule operates to exclude assertions made other than those made by the witness who is testifying as evidence of the truth of what is being asserted. The pure hearsay rule is extremely restrictive and has been extensively modified by various statutory provisions. Thus, there are rules about the proving of documents and business books. Bankers' books have separate legislation. Some of the rules apply explicitly to computers, but many do not, although they can be (and have been) interpreted to cover many situations in which computers are involved.

For example, in the U.K. there have been situations where legal rules presumably designed to help the court may in fact hinder it. In practice, these issues may be circumvented. For instance, in a criminal case, evidence may be obtained by inadmissible methods. This evidence, however, then points investigators to admissible sources of evidence for the same sets of circumstances. An example of this could occur during a fraud investigation. In other words, computer search methods are often used to identify allegedly fraudulent transactions, but the evidential items eventually presented in court are paper-based invoices, contract notes, dockets, or other documents. In this manner, the prosecution can demonstrate to the jury the deception or breach of the Companies Act or other specific fraudulent act. Again, in civil litigation the parties may decide to jointly accept computer-based evidence (or not to challenge it) and instead concentrate on the more substantive elements in the dispute. A defendant may prefer to have a substantive defense rather than a technical one based on inadmissibility. Or, again, the legal team may not feel sufficiently competent to embark on a technical challenge.

In the U.S., many practical problems exist around the actual seizure of computers containing evidence. Law enforcement officers must comply with the Fourth Amendment to the U.S. Constitution.

Subject Matter of Computer Forensics

The subject matter of computer forensics can, thus, not be solely concerned with procedures and methods of handling computers, the hardware from which they are made up, and the files they contain. The ultimate aim of forensic investigation is its use in legal proceedings. At the same time, an obsession with common law and judicial rules is likely to inhibit many investigations. It might be a mistake for inquiries not to be commenced simply because of fear of possible inadmissibility. Furthermore, as we have already seen, a number of computer-investigatory methods may turn out not to be directly admissible but may nevertheless be useful in locating noncomputer evidence that is admissible.

One may have to take a somewhat pragmatic view of the precise bounds of the subject matter, but it should still be possible to define its core activities. It might help to explore the way in which forensic science in general has developed and then see what expectations one might reasonably have of computer forensics.

Although forensic science was already well established, and indeed forms a central feature of many of Conan Doyle's Sherlock Holmes stories published from 1892 onwards, up until the 1970s, each forensic scientist tended to develop his or her own methods and present them ad hoc to juries. Obviously, reliance was placed on descriptions of methods used by others, but for courts, the tests of whether to believe the forensic evidence were the manner of presentation—the supposed eminence of the forensic scientist and the skill of the opposition lawyer (or rival expert who might be called). During the 1970s, a more formal checklist-based approach was introduced. This was partly to bring about standardization as between different laboratories and partly in response to the criticism (in the U.K.) that arose over such controversial cases as the Birmingham Six. In the U.K. Home Office Forensic Service, these checklists were devised by senior staff. Obviously, such checklists are revised in the light of experience—the publication of new specialist research or adverse experience during a trial. An increasingly used feature of modern practice is quality control, which involves work being checked by an otherwise uninvolved coworker before being offered to external scrutiny. In any event, the broad tests for evidence include

Authenticity: Does the material come from where it purports?

Reliability: Can the substance of the story the material tells be believed and is it consistent? In the case of computer-derived material, are there reasons for doubting the correct working of the computer?

Completeness: Is the story that the material purports to tell complete? Are there other stories that the material also tells that might have a bearing on the legal dispute or hearing?

Freedom from interference and contamination: Are these levels acceptable as a result of forensic investigation and other post-event handling [5]?

Any approach to computer forensics would, thus, need to include the elements of

- Well-defined procedures to address the various tasks
- An anticipation of likely criticism of each methodology on the grounds of failure to demonstrate authenticity, reliability, completeness, and possible contamination as a result of the forensic investigation
- The possibility for repeat tests to be carried out, if necessary, by experts hired by the other side
- Checklists to support each methodology
- An anticipation of any problems in formal legal tests of admissibility
- The acceptance that any methods now described would almost certainly be subject to later modification [5]

Divergences from Conventional Forensic Investigation

There will be divergences from the expectations of more traditional areas of forensic investigation. The main reason is the rate of change of computer technology. The devisor of a test for the presence of a prohibited drug, an explosive, fabric fibers, bodily tissues, and the like, can expect that over a period of time, the test may be improved or shown to be defective, but, the need for the test and most of its essential details will probably not change. However, in computers, newness and obsolesce is the norm.

For example, a key feature of computer forensics is the examination of data media: new forms and methods of data storage occur at intervals of less than 4 years. The floppy disk of 13 years ago was in 5.25 inch format and held 360 k. The current equivalent is 3.5 inches and holds 1.44 MB, and much higher densities are expected soon. A typical hard-disk size on a PC of the same date was 20-30 MB, was in 5.25 inch form, and used modified frequency modulation (MFM) controller technology. Today most PCs have hard disks in excess of 1750 MB in 2.5 inch or even 1.5 inch form using integrated development environment (IDE) or run length limited (RLL) technology. On minis and mainframes, data may be held on redundant array of independent (or inexpensive) disks (RAID), where individual files may be split and spread over eight or more separate disk surfaces. Similar changes have taken place in tape technology and the use of erasable programmable read-only memory (EPROMs).

Computer architectures have gone through profound changes in the same short period. PCs have become much more powerful, the large central mainframe is now a rarity, and large companies are now served by a multiplicity of smaller computers that all interact via a complex network.

Computer peripherals keep changing as well. Modems and network routers have become intelligent, and digitizing scanners are fairly common devices. They can be subverted, for example, for forgery.

Wide-area telecom methods are being used more and more. These provide opportunities for both high-tech criminals and forensic investigators. The protocols they use also keep changing.

The foregoing simply lists technological changes. Similar changes have taken place in computer applications; these, in turn, have affected the type of information one might expect to find held in a computer. For example, over the same 13 years, the following technological changes have taken place:

- The growth of email, both locally within large organizations and worldwide.
- The growth of client/server applications.
- The software outcome of the more complex hardware architectures.
- The client/server situation (software on).
- The ability of a PC or small local machine to interact with software and data held on other nonlocal machines and large mainframes in a way that appears to be seamless to the user. One key effect of this is that a computer document often does not exist in some computer equivalent of a filing cabinet, but, rather, is assembled on demand by the activity of one computer drawing information from many others.
- The evidence of a transaction or event may, therefore, only be provable by the presentation of all the records from all the computers involved, plus an explanation of how the assembly of the report relied on took place.
- The greater use of Electronic Data Interchanges (EDIs) and other forms of computer-based orders, bills of lading, payment authorizations, etc. EDIs have very complex structures, with some evidence being held in computers owned by the counter-parties and some by the EDI supplier/regulator.
- Computer graphics: computer-aided design (CAD) methods, particularly those that provide an element of autocompletion or filling-in of basic design ideas.
- More extended, easier-to-use databases.
- The greater use of computer-controlled procedures (sales, dispatch, and emergency services; computer-controlled processes; traffic control; and manufacturing).
- The methods of writing and developing software. There is much greater use of libraries of procedures (of new computer language models). For example, object-oriented programming environments and new, more formal methods of program development; standards and methods of testing have also changed [5].

As a result, computer forensic methods may not have the time in which to establish themselves, or the longevity, that more traditional chemistry- and physics-based forensics enjoy. Nevertheless, the usual way in which specific forensic methods become accepted is via publication in a specialist academic journal. For example, a forensic scientist seeking to justify a methodology in court can do so by stating that it is based on a specific published method that had not up to the point of the hearing been criticized.

NOTE

The rule of best practice refers to the use of the best practice available and known at the time of the giving of evidence.

CASE HISTORIES

One of the fundamental principles of computer investigation is the need to follow established and tested procedures meticulously and methodically throughout the investigation. At no point of the investigation is this more critical than at the stage of initial evidence capture. Reproducibility of evidence is the key. Without the firm base of solid procedures, which have been strictly applied, any subsequent antirepudiation attempts in court will be suspect, and the case as a whole will likely be weakened.

There have been several high-profile cases recently where apparently solid cases have been weakened or thrown out on the basis of inappropriate consideration given to the integrity and reproducibility of the computer evidence. This may happen for several reasons. Lack of training is a prime culprit. If the individuals involved have not been trained to the required standards, or have received no training at all, then tainted or damaged computer evidence is the sad but inevitable result.

Another frequent cause is lack of experience. Not only lack of site experience, but also inappropriate experience of the type of systems, might be encountered. One of the most difficult on-site skills is knowing when to call for help. It is essential that a sympathetic working environment is created such that peer pressure or fear of loss of status and respect does not override the need to call for help. Easier said than done, perhaps, but no less essential for that reason.

Finally, sloppiness, time pressure, pressure applied on-site, fatigue, and carelessness have all been contributory factors in transforming solid computer evidence into a dubious collection of files. These totally avoidable issues are related to individual mental discipline, management control and policy, and selecting appropriate staff to carry out the work. There are issues with which one cannot sympathize. This is bad work, plain and simple.

Ultimately, any time the collection of computer evidence is called into question, it is damaging to everyone who is a computer forensic practitioner; it is in everyone's best interest to ensure that the highest standards are maintained.

To use a rather worn phrase from an old American police series (*Hill Street Blues*): "Let's be careful out there!"

Taken for a Ride

A sad, but all too frequent story, from prospective clients: I've just spent $15,000 on a Web site and got taken for a ride. I cannot find the con man now and all I have is an alias and a pay-as-you-go mobile number. Can you help me please?

What Can You Do?

It is strongly recommended that people dealing with entities on the Internet need to make sure they know who they are dealing with before they enter into any transaction or agreement. If you cannot obtain a real-world address (preferably within the jurisdiction in which you live), then think twice about going any further. Always question the use of mobile phone numbers—they should set alarm bells ringing! This task is made easier in the U.K., as all mobile numbers [6] start with 077xx, 078xx, or 079xx. Pagers start with 076xx. From April 28, 2001, on, all old mobile, pager (those that do not begin 07), special rate, and premium rate numbers stopped working.

If you do want to proceed with the transaction, then use a credit card rather than a debit card or other type of money transfer; then at least you will have some protection and only be liable for $50 rather than having your entire bank account cleaned out. In terms of tracing a suspect like the one in the preceding, your computer forensic experts should be able to trace emails around the world; and, by acting quickly and in conjunction with legal firms, they should be able to track individuals down to their homes. An application for a civil search order can then allow entry and the experts will be able to secure all electronic evidence quickly and efficiently. Internet cafés are sometimes more of a problem, but it is remarkable how many users go to the trouble of trying to disguise their tracks only to end up sitting in exactly the same seat every time they visit the same Café. So, yes, your computer forensic experts can help, but by taking the proper precautions, you would not need to call them in the first place.

Abuse of Power and Position

This message is by no means new; in fact, it could be said that it has been repeated so many times in so many forums that it is amazing that management still falls foul of the following circumstances. In recent months, investigators at Vogon International Limited [7] have been asked to examine computer data for evidence of fraud. On one occasion, the client was a charity, and on the second, a multinational company.

In both cases, fraud, totaling hundreds of thousands of dollars was uncovered. The modus operandi of the suspects was very similar in both cases. Bogus companies were set up and invoices were submitted for payment. The fraudsters were in a position to authorize the payment of the invoices and had the power to prevent unwelcome scrutiny of the accounts.

In addition, one of the fraudsters was paying another member of the staff to turn a blind eye to what was happening. On further investigation, this member of the staff was obviously living beyond his means.

The message is simple: whether you are a multinational company or a small business, the possibility of fraud is ever present. While not wishing to fuel paranoia, traditional checks and balances must be in place to ensure that those trusted members of the staff who have power cannot abuse their positions.

Secure Erasure

Now, let's touch on this "old chestnut" again, because it appears to be the source of considerable confusion and misinformation. Vogon's customer base seems to be polarized into two main camps [7]: those who desperately want to retain their data and fail, often spectacularly, to do so and those who wish to irrevocably destroy their data, and frequently fail in a similarly dramatic manner.

The latter may be criminals who wish to cover their tracks from the police or legitimate business organizations who wish to protect themselves from confidential information falling into the wrong hands. Fundamentally, the issues are the same. The legitimate destruction of data is ultimately a matter of management responsibility, which requires a considered risk analysis to be carried out.

To the question, Can data be securely erased?, the answer is, self-evidently, yes. If you were to ask, Is it straightforward or certain?, it depends, would be the answer.

Many systems are in use for securely erasing data from a wide range of media. Some are effective, some completely ineffective, and some partially effective. It is the latter situation that causes concern and, frequently, not an inconsiderable amount of embarrassment.

Those systems that absolutely destroy data do so in a manner that is total, unequivocal, and final; there can exist no doubt as to their effectiveness. Systems that are sold as being completely effective but that are fundamentally flawed are obviously flawed. With only cursory analysis, this is evident, so these are (or should be) swiftly disregarded.

Vogon is regularly asked to verify the destruction of data by many of their large clients [7]. What they find is that frequently only a fraction of a sample sent is correctly or accurately deleted. RAID systems are a prime candidate for chaos. Certain revisions of drive firmware can present special challenges; in some cases, even the software used defeats the eraser. The list of such software is long and growing.

Vogon is often asked for advice on this issue [7]. The answer is always the same. If the destruction of data has more value than the drive, physically destroy the drive. Crushing is good; melting in a furnace is better. If the drive has more value than the data, what are you worrying about?

CASE STUDIES

Over the years, Vogon's data-recovery laboratories have seen pretty much everything that can happen to a computer, no matter how incredible, whether it is a geologist who, in testing for minerals, inadvertently blew up his own laptop, or the factory worker who covered the computer running the production line in maple syrup. The list is now so long that the incredible has become almost mundane. Fortuitously, two in the latest of a long line of incredible recoveries recently occurred, so, it seemed appropriate to include them as case studies.

Case Study One: The Case of the Flying Laptop

Picture the scene: police rushing into premises on the ninth floor of a building. Almost immediately thereafter, a laptop accelerates rapidly groundward out of the window of the aforementioned premises.

As long ago as 1687, Sir Isaac Newton predicted with uncanny accuracy the inevitable conclusion to this action: namely, the laptop (or to be strictly accurate, large number of pieces of a former laptop) coming to rest with a singular lack of grace on the ground. Luckily, no one was injured by the impact. The resultant bag of smashed laptop components arrived at Vogon's laboratory for a forensically sound data recovery [7].

The laptop computer had impacted the ground across its front edge at an angle, forcing the hard disk drive assembly to go completely through the screen of the laptop. The highly delicate spatial relationship between heads, flexures, platters, and spindle had become disturbed, and the bed of the drive unit was not concave. This imparted an oscillation in two dimensions during drive operation. The drive electronics were destroyed in the impact. After an evening's work by a highly skilled hardware engineer, it was determined that a full fix was possible, and a perfect image was taken. Vogon had no knowledge of whether the chap was guilty, but they bet he was in shock when the evidence was presented [7].

Case Study Two: The Case of the Burned Tapes

This case does not involve true forensic investigation, but it does highlight the fact that it is important never to give up on a job, no matter how seemingly hopeless it appears.

Sets of digital audio tape (DAT) tapes were sent to Vogon from a loss adjuster [7]. The DAT tapes were caught in a fire, which had engulfed a company's head office and wiped out the primary trading infrastructure. The company's IT systems had been at the center of the blaze, and this had unfortunately raised the magnetic media on the surface of the servers hard drives past its curie point. The DAT tapes had, rather inadvisably as it turned out, not been stored off-site. They were, however, stored a little way from the center of the blaze.

Despite this, the DAT tapes arrived in a rather sorry condition. The plastic casing had melted to, around, and onto the tapes, and the whole mechanism was fused into a homologous glob. It is fair to say the tapes were sent to Vogon with the full expectation that they would be declared unrecoverable and used as the basis from which to make a loss settlement [7].

This recovery involved hours of work from both hardware and tape recovery engineers. The tapes were carefully cut away from the molten mass and treated for fire damage. The next stage was to rehouse the tapes and pass them forward to the tape recovery team. Following a number of complex stages, the recovery team was able to extract a stream of data from the tapes that accounted for some 95% of the original data stored on the company's tape backups.

The result was a company up and running in a matter of days rather than weeks, or, more likely, never. It also resulted in a significant reduction in the claims settlement by the loss adjuster and business continuity for the unfortunate company.

SUMMARY

Computers have appeared in the course of litigation for over 28 years. In 1977, there were 291 U.S. federal cases and 246 state cases in which the word *computer* appeared and which were sufficiently important to be noted in the Lexis database. In the U.K., there were only 20. However, as early as 1968, the computer's existence was considered sufficiently important for special provisions to be made in the English Civil Evidence Act.

The following description is designed to summarize the issues rather than attempt to give a complete guide. As far as one can tell, noncontentious cases tend not to be reported, and the arrival of computers in commercial disputes and in criminal cases did not create immediate difficulties. Judges sought to allow computer-based evidence on the basis that it was no different from forms of evidence with which they were already familiar: documents, business books, weighing machines, calculating machines, films, and audio tapes. This is not to say that such cases were without difficulty; however, no completely new principles were required. Quite soon, though, it became apparent that many new situations were arising and that analogies to more traditional evidential material were beginning to break down. Some of these were tackled in legislation, as with the English 1968 act and the U.S. Federal Rules of Evidence in 1976, but many were addressed in a series of court cases. Not all of the key cases deal directly with computers, but they do have a bearing on them as they relate to matters that are characteristic of computer-originated evidence. For example, computer-originated evidence or information that is not immediately readable by a human being is usually gathered by a mechanical counting or weighing instrument. The calculation could also be performed by a mechanical or electronic device.

The focus of most of this legislation and judicial activity was determining the admissibility of the evidence. The common law and legislative rules are those that have arisen as a result of judicial decisions and specific law. They extend beyond mere guidance. They are rules that a court must follow; the thought behind these rules may have been to impose standards and uniformity in helping a court test authenticity, reliability, and completeness. Nevertheless, they have acquired a status of their own and in some cases prevent a court from making ad hoc common sense decisions about the quality of evidence. The usual effect is that once a judge has declared evidence inadmissible (that is, failing to conform to the rules), the evidence is never put to a jury, for a variety of reasons that will become apparent shortly. It is not wholly possible for someone interested in the practical aspects of computer forensics (that is, the issues of demonstrating authenticity, reliability, completeness, or lack thereof) to separate out the legal tests.

Now let’s look at some of the more common questions that computer forensics may be able to answer. The following conclusions are not exhaustive, nor is the order significant.

Conclusions

Documents: To prove authenticity; alternatively, to demonstrate a forgery. This is the direct analogy to proving the authenticity of a print-based document.

Reports: Computer generated from human input. This is the situation where a series of original events or transactions are input by human beings, but where after regular computer processing, a large number of reports, both via print-out and on-screen can be generated. Examples would include the order, sales, and inventory applications used by many commercial organizations and retail banking.

Real evidence: Machine-readable measurements and the like (weighing, counting, or otherwise recording events) and the reading of the contents of magnetic stripes and bar codes and smart cards.

Reports generated from machine-readable measurements: Items that have been counted, weighed, and so on and the results then processed and collated.

Electronic transactions: To prove that a transaction took place or to demonstrate a presumption was incorrect. Typical examples include money transfers, ATM transactions, securities settlement, and EDIs.

Conclusions reached by search programs: These are programs that have searched documents, reports, and so on, for names and patterns. Typical users of such programs are auditors and investigators.

Event reconstruction: To show a sequence of events or transactions passing through a complex computer system. This is related to the proving of electronic transactions, but with more proactive means of investigation event reconstruction—to show how a computer installation or process dependent on a computer may have failed. Typical examples include computer contract disputes (when a computer failed to deliver acceptable levels of service and blame must be apportioned), disaster investigations, and failed trade situations in securities dealing systems.

Liability in a situation: This is where CAD designs have relied on autocompletion or filling-in by a program (in other respects, a CAD design is a straightforward computer-held document). Liability in a situation is also where a computer program has made a decision (or recommendation) based on the application of rules and formulae, where the legal issue is the quality and reliability of the application program, and the rules with which it has been fed.

The following occasions could arise in any of a number of forms of litigation:

- Civil matters
- Breach of contract
- Asset recovery
- Tort, including negligence
- Breach of confidence
- Defamation
- Breach of securities industry legislation and regulation or companies acts
- Employee disputes
- Copyright and other intellectual property disputes
- Consumer protection law obligations (and other examples of no-fault liability)
- Data protection legislation
- Criminal matters such as
  - Theft acts, including deception
  - Criminal damage
  - Demanding money with menaces
  - Companies law, securities industry, and banking offenses
  - Criminal offenses concerned with copyright and intellectual property

- Drug offenses
- Trading standards offenses
- Official secrets
- Computer Misuse Act offenses
- Pornography offenses

As mentioned earlier, the most likely situations are that computer-based evidence contributes to an investigation or to litigation and is not the whole of it.

An Agenda for Action

When completing the Principle Forensic Activities Checklist (as shown in Table F1.2 of Appendix F), the computer forensics specialist should adhere to the provisional list of actions for some of the principle forensic methods. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these methods have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and an optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Criminal prosecutors use computer evidence in a variety of crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.
2. True or False? Civil litigations cannot make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases.
3. True or False? Insurance companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.
4. True or False? Corporations often hire computer forensics specialists to find evidence relating to sexual harassment, embezzlement, theft or misappropriation of trade secrets, and other internal and confidential information.
5. True or False? Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of computer equipment.

Multiple Choice

1. When handling computers for legal purposes, investigators increasingly are faced with four main types of problems, except:
   A. How to recover data from computers while preserving evidential integrity
   B. How to keep your data and information safe from theft or accidental loss
   C. How to securely store and handle recovered data
   D. How to find the significant information in a large volume of data
   E. How to present the information to a court of law and to defense during disclosure
2. In order for a double tier approach to work it is necessary to have:
   A. A defined methodology
   B. Civil control
   C. A breach of contract
   D. Asset recovery
   E. Tort, including negligence
3. Criteria for equipment in the double tier approach results in the following except:
   A. Simple to use
   B. Quick to learn
   C. Totally reliable
   D. Robust and durable
   E. Legally operable
4. A computer forensics specialist is the person responsible for doing computer forensics. The computer forensics specialist will take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject computer system. This results in the following steps except:
   A. Protects the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction
   B. Discovers all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files
   C. Recovers all (or as much as possible) of discovered deleted files
   D. Reconstructs system failure
   E. Reveals (to the extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system

5. A computer forensics professional does more than turn on a computer, make a directory listing, and search through files. Your forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case. For example, they should be able to perform the following services, except:
   A. Data seizure
   B. Data duplication and preservation
   C. Data recovery
   D. Document searches
   E. Data dump

Exercise

When senior officials of a Fortune 500 company found out that certain employees were operating internal slush funds totaling about $286 million dollars, they called in a computer forensics professional to find out why and to assess the impact. Please explain how the computer forensics professional went about resolving the problem.

HANDS-ON PROJECTS

A major hotel and casino needed to preserve legacy client digital linear tape (DLT) tapes and recover, extract, and host over 260 gigabytes of electronic data for attorney review. How would your computer forensics team go about preserving and recovering the electronic data?

Case Project

Let's look at a real-world scenario and how computer forensics plays into it. Late one night, a system administrator (sysadmin) troubleshoots a network problem. She captures several minutes worth of network traffic to review with a protocol analyzer. While conducting this review, she notices some odd traffic. A user's desktop has sent a well-formed packet to an obscure port on an unfamiliar IP address outside the company's firewall. Shortly thereafter, one of the company's research and development database servers transmits a packet that does not conform to any of the formats the company uses to the same IP address. This intrigues the sysadmin, who does a lookup of the IP address; it comes back as one of the firm's competitors. Now, she's not merely curious, she's concerned. She picks up the phone and calls her boss. The boss could say, "Just block that port," and then go back to bed, but there's a far better way to handle this situation. Please explain how you would handle this situation.

Optional Team Case Project

A major energy services provider was faced with a request from the Securities and Exchange Commission to provide copies of all electronic correspondence within the company and its subsidiaries worldwide relating to key projects. How do you as a computer forensics specialist handle this?

REFERENCES

[1] "2003 Computer Crime and Security Survey," Federal Bureau of Investigation, J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW, Washington, D.C. 20535-0001, 2003.

[2] Robbins, Judd, "An Explanation of Computer Forensics," National Forensics Center, 774 Mays Blvd. #10 143, Incline Village, NV 89451, 2004 [The Computer Forensics Expert Witness Network, 472 Scenic Drive, Ashland, OR] (©2004, National Forensics Center. All rights reserved), 2001.

[3] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

[4] "Computer Forensics," Rehman Technology Services, Inc., 18950 U.S. Highway 441, Suite 201, Mount Dora, Florida 32757, 2001. (©2002, Rehman Technology Services, Inc. All rights reserved), 2001.

[5] Sommer, Peter, "Computer Forensics: An Introduction," Virtual City Associates, PO Box 6447, London N4 4RX, United Kingdom, 2001. *http://csrc.lse.ac.uk.*

[6] Vacca, John R., *i-mode CrashCourse*, McGraw-Hill, New York, 2001.

[7] *Vogon Forensics Bulletin,* Vol. 3, Issue 3, Vogon International Limited, Talisman Business Centre, Talisman Road, Bicester, Oxfordshire, OX26 6HR United Kingdom, 2001.

2 Types of Computer Forensics Technology

Defensive information technology will ultimately benefit from the availability of cyber forensic evidence of malicious activity. Criminal investigators rely on recognized scientific forensic disciplines, such as medical pathology, to provide vital information used in apprehending criminals and determining their motives. Today, an increased opportunity for cyber crime exists, making advances in the law enforcement, legal, and forensic computing technical arenas imperative. As previously explained, cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media, and computer peripherals that allow investigators to solve a crime. Cyber forensics focuses on real-time, online evidence gathering rather than the traditional offline computer disk forensic technology.

Two distinct components exist in the emerging field of cyber forensics technology. The first, computer forensics, deals with gathering evidence from computer media seized at the crime scene. Principal concerns with computer forensics involve imaging storage media, recovering deleted files, searching slack and free space, and preserving the collected information for litigation purposes. Several computer forensic tools are available to investigators. The second component, network forensics, is a more technically challenging aspect of cyber forensics. It involves gathering digital evidence that is distributed across large-scale, complex networks. Often this evidence is transient in nature and is not preserved within permanent storage media. Network forensics deals primarily with in-depth analysis of computer network intrusion evidence, because current commercial intrusion analysis tools are inadequate to deal with today's networked, distributed environments.

Similar to traditional medical forensics, such as pathology, today's computer forensics is generally performed postmortem (after the crime or event occurred). In a networked, distributed environment, it is imperative to perform forensic-like examinations of victim information systems on an almost continuous basis, in addition to traditional postmortem forensic analysis. This is essential to continued functioning of critical information systems and infrastructures. Few, if any, forensic tools are available to assist in preempting the attacks or locating the perpetrators. In the battle against malicious hackers, investigators must perform cyber forensic functions in support of various objectives. These objectives include timely cyberattack containment, perpetrator location and identification, damage mitigation, and recovery initiation in the case of a crippled, yet still functioning, network. Standard intrusion analysis includes examination of many sources of data evidence (intrusion detection system logs, firewall logs, audit trails, and network management information). Cyber forensics adds inspection of transient and other frequently overlooked elements such as contents or state of memory, registers, basic input/output system, input/output buffers, serial receive buffers, L2 cache, front side and back side system caches, and various system buffers (drive and video buffers).

Now let's briefly look at specific types of computer forensics technology that are being used by military, law enforcement, and business computer specialists. It is beyond the scope of this chapter to cover in detail every type of computer forensic technology. The following chapters of the book as well as the appendixes have been designed and created to do that specific task.

TYPES OF MILITARY COMPUTER FORENSIC TECHNOLOGY

The U.S. Department of Defense (DoD) cyber forensics includes evaluation and in-depth examination of data related to both the trans- and post-cyberattack periods. Key objectives of cyber forensics include rapid discovery of evidence, estimation of potential impact of the malicious activity on the victim, and assessment of the intent and identity of the perpetrator. Real-time tracking of potentially malicious activity is especially difficult when the pertinent information has been intentionally hidden, destroyed, or modified in order to elude discovery. The information directorate's cyber forensic concepts are new and untested. The directorate entered into a partnership with the National Institute of Justice via the auspices of the National Law Enforcement and Corrections Technology Center (NLECTC) located in Rome, New York, to test these new ideas and prototype tools. The Computer Forensics Experiment 2000 (CFX-2000) resulted from this partnership. This first-of-a-kind event represents a new paradigm for transitioning cyber forensic technology from military research and development (R&D) laboratories into the hands of law enforcement. The experiment used a realistic cyber crime scenario specifically designed to exercise and show the value added of the directorate-developed cyber forensic technology.

The central hypothesis of CFX-2000 is that it is possible to accurately determine the motives, intent, targets, sophistication, identity, and location of cyber criminals and cyber terrorists by deploying an integrated forensic analysis framework. The execution of CFX-2000 required the development and simulation of a realistic, complex cyber crime scenario exercising conventional, as well as R&D prototype, cyber forensic tools.

The NLECTC assembled a diverse group of computer crime investigators from DoD and federal, state, and local law enforcement to participate in the CFX-2000 exercise hosted by the New York State Police's Forensic Investigative Center in Albany, New York. Officials divided the participants into three teams. Each team received an identical set of software tools and was presented with identical initial evidence of suspicious activity. The objective of each team was to uncover several linked criminal activities from a maze of about 30 milestones that culminated in an information warfare crime (Figure 2.1) [1].

The cyber forensic tools involved in CFX-2000 consisted of commercial off-the-shelf software and directorate-sponsored R&D prototypes. The Synthesizing Information from Forensic Investigations (SI-FI) integration environment, developed under contract by WetStone Technologies, Inc. [2], was the cornerstone of the technology demonstrated. SI-FI supports the collection, examination, and analysis processes employed during a cyber forensic investigation. The SI-FI prototype uses digital evidence bags (DEBs), which are secure and tamperproof *containers* used to store digital evidence. Investigators can seal evidence in the DEBs and use the SI-FI implementation to collaborate on complex investigations. Authorized users can securely reopen the DEBs for examination, while automatic audit of all actions ensures the continued integrity of their contents. The teams used other forensic tools and prototypes to collect and analyze specific features of the

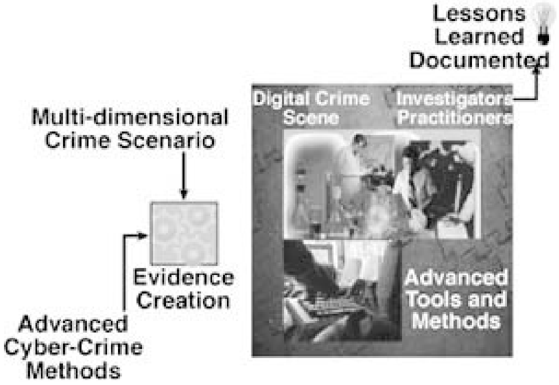

Lessons
Learned
Documented
Digital Crime Scene
Investigators Practitioners
Multi-dimensional Crime Scenario
Evidence Creation
Advanced Cyber-Crime Methods
Advanced Tools and Methods

FIGURE 2.1 CFX-2000 schematic (© 2002, Associated Business Publications. All rights reserved).

digital evidence, perform case management and timelining of digital events, automate event link analysis, and perform steganography detection. The results of CFX-2000 verified that the hypothesis was largely correct and that it is possible to ascertain the intent and identity of cyber criminals. As electronic technology continues its explosive growth, researchers need to continue vigorous R&D of cyber forensic technology in preparation for the onslaught of cyber reconnaissance probes and attacks.

TYPES OF LAW ENFORCEMENT COMPUTER FORENSIC TECHNOLOGY

As previously defined, computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored in the form of magnetically encoded information (data). Often the computer evidence was created transparently by the computer's operating system and without the knowledge of the computer operator. Such information may actually be hidden from view and, thus, special forensic software tools and techniques are required to preserve, identify, extract, and document the related computer evidence.

Computer forensics tools and techniques have proven to be a valuable resource for law enforcement in the identification of leads and in the processing of computer-related evidence. Computer forensics tools and techniques have become important resources for use in internal investigations, civil lawsuits, and computer security risk management.

Forensic software tools and methods can be used to identify passwords, logons, and other information that is automatically dumped from the computer memory as a transparent operation of today's popular personal computer operating systems. Such computer forensic software tools can also be used to identify backdated files and to tie a diskette to the computer that created it.

Law enforcement and military agencies have been involved in processing computer evidence for years. This section touches very briefly on issues dealing with Windows NT®, Windows® 2000, XP and 2003 and their use within law enforcement computer forensic technology.

Windows XP and Windows 2003 are operating systems that are often used on notebook and desktop computers in corporations and government agencies. Thus, they are currently the operating systems most likely to be encountered in computer investigations and computer security reviews. Be advised that this chapter does not cover the use of *black box* computer forensics software tools. Those tools are good for some basic investigation tasks, but they do not offer a full computer forensics solution. Furthermore, such approaches are all but useless in computer security risk assessments. Such assessments usually require that searches and file listings be conducted overtly or even covertly from a single floppy diskette.

Computer Evidence Processing Procedures

Processing procedures and methodologies should conform to federal computer evidence processing standards. Computer processing procedures have also been developed for the U.S. Treasury Department.

Training and certification programs have also been developed for the International Association of Computer Investigation Specialists (IACIS). For these reasons, computer forensic trainers and instructors should be well qualified to teach the correct computer-processing methods and procedures.

Preservation of Evidence

Computer evidence is fragile and susceptible to alteration or erasure by any number of occurrences. Computer forensic instructors should expose their trainees to bit stream backup theories that ensure the preservation of all storage levels that may contain evidence. For example, SafeBack software overcomes some of the evidence weaknesses inherent in black box computer forensics approaches (see sidebar, “Mirror Image Backup Software”). SafeBack technology can be purchased from New Technologies, Inc. [3] and has become a worldwide standard in making mirror image backups since 1990, when it was developed based on requirements then established by the U.S. Treasury Department and the IACIS.

MIRROR IMAGE BACKUP SOFTWARE

SafeBack is used to create mirror-image (bit-stream) backup files of hard disks or to make a mirror-image copy of an entire hard disk drive or partition. The process is analogous to photography and the creation of a photo negative. Once the photo negative has been made, several exact reproductions can be made of the original. Unlike a photo, SafeBack image files cannot be altered or modified to alter the reproduction. This is because SafeBack is an industry standard self-authenticating computer forensics tool that is used to create evidence-grade backups of hard drives.

With the release of SafeBack version 3.0 or higher, the integrity of SafeBack files is maintained through the use of two separate mathematical hashing processes that rely upon the National Institute of Standards and Technology (NIST)-tested Secure Hash Algorithm256 (SHA256). Users of prior versions of SafeBack are encouraged to upgrade to take advantage of the greater levels of accuracy achieved with version 3.0. Information about upgrades can be found on the Internet at *http://www.forensics-intl.com/*. The upgrade of SafeBack has new and added features and it takes into account the last sector error finding by NIST concerning the older SafeBack version 2.0.

CAUTION *URLs are subject to change without notice.*

→

Backup image files created with SafeBack can be written to any writable magnetic storage device, including small computer system interface (SCSI) tape backup units. SafeBack preserves all the data on a backed-up or copied hard disk, including inactive or deleted data. Backup image files can be restored to another system's hard disk. Remote operation via a parallel port connection allows the hard disk on a remote PC to be read or written by the master system. A date- and time-stamped audit trail maintains a record of SafeBack operations during a session, and when the default is used an SHA256 hash is recorded in the output audit file. This hash can be used to cross-validate the accuracy of the process with any other software utility that relies upon the NIST-tested SHA256 algorithm. To avoid possible claims that the SafeBack image file may have been altered after the fact, SafeBack now safeguards the internally stored SHA256 values. Any alterations of computer data are quickly brought to the attention of the operator of the program when the SafeBack image file is restored.

Simply put, SafeBack is a DOS-based utility used to back up and restore hard disks. SafeBack picks up every last bit of data-unused and erased data included—on the original disk and stores it in a tape or disk file (or series of files). SafeBack can take that same backup file and recreate the original disk on your own system. SafeBack does not write or otherwise modify the original system and can (and should) be started from a boot diskette.

SafeBack also has a couple of *derivative* operating modes. The first is Verify mode, where restoring from a backup disk is done, but the data is thrown away. This is more useful than it first appears to be because it allows the operator of the program to scan his or her backups to make sure that they will read back without errors, without having to go through the setup required by a standard SafeBack restore procedure. The other derivative operation is Copy, which feeds the Restore function directly with the output of the Backup function, with no intermediate files. This is less useful than it first appears to be. If the operator of SafeBack is considering making a copy, he might as well make a backup image file and then restore it as needed.

Primary Uses

The primary uses of SafeBack are as follows:

- Used to create evidence-grade backups of hard disk drives on Intel-based computer systems
- Used to exactly restore archived SafeBack images to another computer hard disk drive of equal or larger storage capacity
- Used as an evidence preservation tool in law enforcement and civil litigation matters
- Used as an intelligence gathering tool by military agencies

→

Program Features and Benefits

The program features and benefits of SafeBack are as follows:

- DOS based for ease of operation, for speed, and to eliminate the problems created by a separate operating system concerning the potential alteration of data.
- No software dongle. Software dongles get in the way and they restrict your ability to process several computers at the same time.
- Incorporates two separate implementations of the NIST-tested SHA256 algorithm to ensure the integrity of all data contained on the target computer storage device.
- Provides a detailed audit trail of the backup process for evidence documentation purposes, and the SafeBack default outputs an SHA256 hash value that can be compared with other utilities when cross-validation of findings are deemed to be important.
- Checks for possible data hiding when sector cyclic redundancy checks (CRCs) do not match on the target hard disk drive. These findings are automatically recorded in the SafeBack audit log file.
- Accurately copies all areas of the hard disk drive.
- Allows the archive of non-DOS and non-Windows hard disk drives (Unix on an Intel-based computer system).
- Allows for the backup process to be made via the printer port.
- Duplicate copies of hard disk drives can be made from hard disk to hard disk in direct mode.
- SafeBack image files can be stored as one large file or separate files of fixed sizes. This feature is helpful in making copies for archive on CDs.
- Uses tried and proven evidence preservation technology with a long-term legacy of success in government agencies.
- Does not compress relevant data to avoid legal arguments that the original computer evidence was altered through data compression or software translation.
- It is fast and efficient. In spite of the extensive mathematical validation, the latest version of SafeBack runs as fast or faster than prior versions. Processing speeds are much faster when state-of-the-art computer systems are used to make the backup.
- Makes copies in either physical or logical mode at the option of the user.
- Copies and restores multiple partitions containing one or more operating systems.
- Can be used to accurately copy and restore most hard disk drives including Windows NT, Windows 2000, and Windows XP configured drives.
- Accuracy is guaranteed in the backup process through the combination of mathematical CRCs that provides a level of accuracy that far exceeds the accuracy provided by 128-bit CRCs (RSA MD5).

→

- Writes to SCSI tape backup units or hard disk drives at the option of the user.
- The current version of SafeBack compresses unused and unformatted sections of the hard disk drive to increase processing speeds and to conserve storage space concerning the writing of the SafeBack image file [3].

Trojan Horse Programs

The need to preserve the computer evidence before processing a computer should be clearly demonstrated by the computer forensic instructor through the use of programs designed to destroy data and modify the operating systems. The participant should be able to demonstrate his or her ability to avoid destructive programs and traps that can be planted by computer users bent on destroying data and evidence. Such programs can also be used to covertly capture sensitive information, passwords, and network logons.

Computer Forensics Documentation

The documentation of forensic processing methodologies and findings is important. This is even true concerning computer security risk assessments and internal audits, because without proper documentation, it is difficult to present findings. If the security or audit findings become the object of a lawsuit or a criminal investigation, then documentation becomes even more important. Thus, the computer forensic instructor should also teach the participant the ins and outs of computer evidence processing methodology (which facilitates good evidence-processing documentation and good evidence chain of custody procedures). The benefits will be obvious to investigators, but they will also become clear to internal auditors and computer security specialists.

File Slack

The occurrence of random memory dumps in hidden storage areas should be discussed and covered in detail during workshops. Techniques and automated tools that are used to capture and evaluate file slack should be demonstrated in a training course. Such data is the source of potential security leaks regarding passwords, network logons, email, database entries, and word processing documents. These security and evidence issues should also be discussed and demonstrated during the training course. The participants should be able to demonstrate their ability to deal with slack and should demonstrate proficiency in searching file slack, documenting their findings, and eliminating the security risk.

Data-Hiding Techniques

Trade secret information and other sensitive data can easily be secreted using any number of techniques. It is possible to hide diskettes within diskettes and to hide entire computer hard disk drive partitions. These issues should be discussed in any computer forensics training course from a detection standpoint, as well as from a security risk standpoint. Tools that help in the identification of such anomalies should be demonstrated and discussed (like AnaDisk^{TM} [see sidebar, "AnaDisk Diskette Analysis Tool"]) in the training course. Participants should be required to demonstrate their understanding of such issues. This aspect of the training becomes especially important during the last day of the course when the participants are called on to extract their Certificate of Completion from a *special* floppy diskette. Data-hiding courses are only open to classified government agencies and businesses that have a demonstrated need to know about this kind of information as outlined in a company's training policies. This is because the information covered in a data-hiding course can be used to defeat government computer security review processes and techniques.

ANADISK DISKETTE ANALYSIS TOOL

AnaDisk turns your PC into a sophisticated diskette analysis tool. The software was originally created to meet the needs of the U.S. Treasury Department in 1991. It is primarily used to identify data storage anomalies on floppy diskettes and generic hardware in the form of floppy disk controllers; bios are needed when using this software. It works at a very low level and makes maximum use of the floppy diskette hardware. The software also has limited search capabilities and can be used to copy abnormal diskettes. It can also be used to write data at a physical sector level and to format diskettes using any number of combinations.

AnaDisk has the capability to duplicate floppy diskettes, but this feature is used primarily with odd diskette formats (in cases like the FBI Russian mole case of suspected spy Robert Phillip Hanssen). However, standard duplication of floppy diskettes is more easily accomplished with New Technology Inc.'s CopyQM (see sidebar "CopyQM: Diskette Duplication Software"), which has been upgraded and certified by the U.S. DoD for making copies of diskettes used in classified computer security risk reviews.

In other words, AnaDisk can be used to analyze floppy diskettes when doing computer evidence consulting work, which involves abnormal floppy diskettes or data storage issues tied to floppy diskettes. It can also be used in data-hiding courses to create data-hiding areas by adding extra sectors and tracks to floppy diskettes and in writing data to unformatted floppy diskettes.

→

Primary Uses

- Security reviews of floppy diskettes for storage anomalies
- Duplication of diskettes that are nonstandard or that involve storage anomalies
- Editing diskettes at a physical sector level
- Searching for data on floppy diskettes in traditional and nontraditional storage areas
- Formatting diskettes in nontraditional ways for training purposes and to illustrate data-hiding techniques

Program Features and Benefits

- DOS-based for ease of operation and speed.
- No software dongle. Again, software dongles get in the way and they are restrictive.
- Keyword searches can be conducted at a very low level and on diskettes that have been formatted with extra tracks. This feature is helpful in the evaluation of diskettes that may involve sophisticated data-hiding techniques.
- All DOS formats are supported, as well as many non-DOS formats (Apple Macintosh, Unix TAR^{TM}, and many others. If the diskette will fit in a PC floppy diskette drive, it is likely that AnaDisk can be used to analyze it.
- Allows custom formatting of diskettes with extra tracks and sectors.
- Scans for anomalies will identify odd formats, extra tracks, and extra sectors. Data mismatches, concerning some file formats, are also identified when file extensions have been changed in an attempt to hide data.
- This software can be used to copy almost any diskette, including most copy-protected diskettes [4].

COPYQM: DISKETTE DUPLICATION SOFTWARE

CopyQM Plus essentially turns a personal computer into a diskette duplicator. In a single pass, diskettes are formatted, copied, and verified. This capability is useful for computer forensics specialists and computer security specialists who need to preconfigure floppy diskettes for specific uses and duplicate them.

Classified government agencies and government contractors are required to perform periodic examinations of government computer systems to determine if

→

classified data may reside on nonclassified computer systems. Programs like New Technology Inc.'s TextSearch Plus (see sidebar, "Text Search Plus") and TextSearch NT were designed specifically for this purpose and they are both certified by the U.S. DoD for use in classified government risk assessments. CopyQM is also certified by the U.S. DoD for use in the duplication of "search disks" used in classified U.S. government computer risk reviews.

CopyQM Plus can also create self-extracting executable programs that can be used to duplicate specific diskettes. This feature makes CopyQM an ideal tool for use in security reviews because once a CopyQM disk-creation program has been created, it can be used by anyone to create pre-configured security risk assessment diskettes. When the resulting program is run, the diskette image of the original diskette will be restored on multiple diskettes automatically.

This process requires little technical knowledge and it allows computer specialists to delegate more of the security risk assessment responsibilities to employees with minimal technical knowledge. The diskette images can also be password protected when the diskette images are converted to self-extracting programs. This is helpful when you want to keep computer forensic and computer security software tools away from curious hands.

Primary Uses

- The program is used to archive the image of a floppy diskette and to create one or more duplicate copies of the master diskette when desired.
- It can be used to make one or more copies of all areas of a *normal* floppy diskette. Thus, it basically turns your PC into a diskette duplication machine. This can be helpful when you need to repeatedly make copies of diskettes for training classes. It is also helpful for making multiple copies of evidence diskettes.
- It can be used to automatically create and serialize software stored on floppy diskettes. This type of *branding* can be helpful in creating copies of diskettes that will be shared among several lawyers or with the court.
- CopyQM Plus can be used to password protect the contents of an entire floppy diskette. This is helpful when diskettes are shared over the Internet and when security is a concern.
- CopyQM Plus can be used to create virus-scanned floppy diskette tool kits configured for repeated tasks performed by computer forensics specialists, electronic data personnel (EDP), auditors and computer security specialists. The software is particularly helpful in creating computer incident response tool kit diskettes.
- CopyQM Plus can be used to send a normal diskette over the Internet.

→

Program Features and Benefits

- DOS-based for ease of operation and speed.
- No software dongle. Again, software dongles get in the way.
- It converts diskettes into self-contained programs that, when executed, recreate the original master diskette as many times as desired.
- All DOS formats are supported as well as many non-DOS formats (Apple Macintosh, Unix TAR, and many others).
- Images may be optionally password protected through the use of built-in encryption.
- Diskette images can be serial numbered anywhere in the copy of the diskette. When this feature is selected, a log of the process is maintained for reference.
- The software can be used to create copy protection (tied to software), making it impossible for a casual pirate to make illegal copies of the software.
- CopyQM Plus is significantly faster than DOS DiskCopy and it automatically copies the subject diskette, verifies the copy, and formats the target diskette during the restoration process.
- It converts one diskette format to another (720 Kbps to 1.44 MB). This feature deals with 360 Kbps, 720 Kbps, 1.2 MB, 1.44 MB, 1.68 MB, and 2.88 MB formats.
- CopyQM Plus can be used to duplicate and restore any number of copies of a given master diskette.
- It copies files, file slack, and unallocated storage space (erased files). It does not copy all areas of copy protected diskettes (extra sectors added to one or more tracks on a floppy diskette). AnaDisk software should be used for this purpose [8].

E-Commerce Investigations

A new Internet *forensic tool* has recently been introduced that aims to help educators, police, and other law enforcement officials trace the past World Wide Web activity of computer users. Net Threat Analyzer^{TM}, from Gresham, Oregon-based New Technology Inc. (NTI), can be used to identify past Internet browsing and email activity done through specific computers. The software analyzes a computer's disk drives and other storage areas that are generally unknown to or beyond the reach of most general computer users.

Kids can figure out ways to prevent their parents from finding anything on their machine, but Net Threat Analyzer goes back in after the fact where things are easier to detect. New Technology Inc. has made its Net Threat Analyzer available free of charge to computer crime specialists, school officials, and police.

The program is booted from a floppy disk and uses filtering tools to collect data on users' basic browsing and email history. It flags possible threats, such as anything dealing with drugs, bombs, country codes, or pornography. Web sites change so often that it's difficult to keep up with which ones are porn or drug sites.

For example, *http://www.whitehouse.gov*, is the official White House Web site, and *www.whitehouse.com* is a pornography site. If Junior's been to whitehouse.com 500 to 700 times, it will make it through most net nanny software, but it will raise a red flag with the Net Threat Analyzer.

The software was designed to help prevent situations like the tragedies at Columbine High School in Littleton, Colorado, and Thurston High School in Springfield, Oregon, where weapons were made by teenagers who had downloaded the instructions from the Internet.

New Technology Inc., which specializes in computer forensics tools and training, has posted order forms for its software on its Web site at *http://www.forensics-intl.com*. The tool is not available to the public, but a special version can be purchased by Fortune 500 companies, government agencies, military agencies, and consultants who have a legitimate need for the software.

Dual-Purpose Programs

Programs can be designed to perform multiple processes and tasks at the same time. They can also be designed for delayed tasking. These concepts should be demonstrated to the training participants during the course through the use of specialized software. The participant should also have hands-on experience with these programs.

Text Search Techniques

New Technology Inc. has also developed specialized search techniques and tools that can be used to find targeted strings of text in files, file slack, unallocated file space, and Windows swap files. Each participant will leave their training class with a licensed copy of their TextSearch Plus™ software and the necessary knowledge to conduct computer security reviews and computer related investigations (see sidebar, "Text Search Plus").

This search tool is approved for use in security reviews by some U.S. government classified agencies.

TEXT SEARCH PLUS

TextSearch Plus was specifically designed and enhanced for speed and accuracy in security reviews. It is widely used by classified government agencies and corporations that support these agencies. The software is also used by hundreds of law enforcement agencies throughout the world in computer crime investigations.

This software is used to quickly search hard disk drives, zip disks, and floppy diskettes for key words or specific patterns of text. It operates at either a logical or physical level at the option of the user. TextSearch Plus has been specifically designed to meet the requirements of the government for use in computer security exit reviews from classified government facilities. The current version is approximately 25% faster than prior versions. It is also compatible with FAT 12, FAT 16, and FAT 32 DOS-based systems. As a result, it can be used on Windows 98, 2000, XP, and 2003 systems. Tests indicate that this tool finds more text strings than any other forensic search tool. It is sold separately and is also included in several of the New Technology Inc. tool suites. As a stand alone tool, it is ideal for security risk assessments. When security spills are identified, they can easily be eliminated with New Technology Inc.'s M-Sweep^{TM} program.

Primary Uses

- Used to find occurrences of words or strings of text in data stored in files, slack, and unallocated file space
- Used in exit reviews of computer storage media from classified facilities
- Used to identify data leakage of classified information on nonclassified computer systems
- Used in internal audits to identify violations of corporate policy
- Used by Fortune 500 corporations, government contractors, and government agencies in security reviews and security risk assessments
- Used in corporate due diligence efforts regarding proposed mergers
- Used to find occurrences of keywords strings of text in data found at a physical sector level
- Used to find evidence in corporate, civil, and criminal investigations that involve computer-related evidence
- Used to find embedded text in formatted word processing documents (WordPerfect^{TM} and fragments of such documents in ambient data storage areas)

→

Program Features and Benefits

- DOS-based for ease of operation and speed.
- No software dongle. Software dongles get in the way and they restrict your ability to process several computers at the same time.
- Small memory foot print (under 60 KB), which allows the software to run on even the original IBM PC.
- Compact program size, which easily fits on one floppy diskette with other forensic software utilities.
- Searches files, slack, and erased space in one fast operation.
- Has logical and physical search options that maintain compatibility with government security review requirements.
- User-defined search configuration feature.
- User configuration is automatically saved for future use.
- Embedded words and strings of text are found in word processing files.
- Alert for graphic files (secrets can be hidden in them).
- Alert for compressed files.
- High speed operation. This is the fastest tool on the market, which makes for quick searches on huge hard disk drives
- Screen and file output.
- False hits don't stop processing.
- Government tested—specifically designed for security reviews in classified environments.
- Currently used by hundreds of law enforcement computer crime units.
- Currently in use by all of the Big 5 accounting firms.
- Currently used by several government military and intelligence agencies.
- Currently used by numerous Fortune 500 corporations.
- The current version allows for up to 120 search strings to be searched for at one time [5].

Fuzzy Logic Tools Used to Identify Unknown Text

New Technology Inc. has also developed a methodology and tools that aid in the identification of relevant evidence and *unknown* strings of text. Traditional computer evidence searches require that the computer specialist know what is being searched for. However, many times not all is known about what may be stored on a given computer system. In such cases, fuzzy logic tools can provide valuable leads as to how the subject computer was used. The training participants should be able to fully understand these methods and techniques. They should also be able to demonstrate their ability to use them to identify leads in file slack, unallocated file space, and Windows swap files. Each training participant should also leave the class with a licensed copy of New Technology Inc.'s Filter_G^{TM} software (see sidebar, "Intelligent Forensic Filter").

INTELLIGENT FORENSIC FILTER

This forensic filter utility is used to quickly make sense of nonsense in the analysis of ambient data sources (Windows swap/page files, file slack, and data associated with erased files). Filter_G is a unique fuzzy logic filter that was awarded patent number 6,345,283 by the U.S. Patent Office. It is used to quickly identify patterns of English language grammar in ambient data files. Such an analysis can be helpful in making quick assessments about how a specific computer was used and the nature of prior English language communications that were involved in the past uses of a subject computer. The program can be used as a sampling tool and it is particularly useful when used to evaluate Windows swap/page files.

Be aware that the functionality of this software was contained in New Technology Inc.'s Filter_I prior to March, 2003. Since that time the functionality was substantially enhanced and incorporated into this program as a stand-alone utility.

PRIMARY USES

- Used as an intelligence gathering tool for quick assessments of a Windows swap/page file to identify past communications on a targeted computer
- Used as a data sampling tool in law enforcement, military, and corporate investigations
- Used to quickly identify patterns of English language grammar in ambient data sources
- Used to identify English language communications in erased file space

PROGRAM FEATURES AND BENEFITS

- DOS-based for speed.
- No software dongle.

→

- Automatically processes any data object (a swap file, a file constructed from combined file slack, a file constructed from combined unallocated space, or a Windows swap/page file.
- Provides output in an ASCII text format that is ready for import into any word processing application, Windows NotePad, or even the DOS Edit program.
- Can be operated in batch mode with other forensic tools and processes.
- Operates at a high rate of speed, and depending upon the CPU involved the software has the capability of processing more than 2 million bytes of data per second.
- Capable of quickly processing ambient data files that are up to 2 gigabytes in size.
- Free upgrades for one year from the date of purchase.
- Quantity discounts and site licenses are available [6].

Disk Structure

Participants should be able to leave a training course with a good understanding of how computer hard disks and floppy diskettes are structured and how computer evidence can reside at various levels within the structure of the disk. They should also demonstrate their knowledge of how to modify the structure and hide data in obscure places on floppy diskettes and hard disk drives.

Data Encryption

A computer forensics course should cover, in general, how data is encrypted; it should also illustrate the differences between good encryption and bad encryption. Furthermore, demonstrations of password-recovery software should be given regarding encrypted WordPerfect, Excel, Lotus, Microsoft Word, and PKZIP files. The participant should become familiar with the use of software to *crack* security associated with these different file structures.

Matching a Diskette to a Computer

New Technology Inc. has also developed specialized techniques and tools that make it possible to conclusively tie a diskette to a computer that was used to create or edit files stored on it. Unlike some *special* government agencies, New Technology Inc. relies on logical rather than physical data storage areas to demonstrate this technique. Each participant is taught how to use special software tools to complete this process.

Data Compression

The participant should be shown how compression works and how compression programs can be used to hide and disguise sensitive data. Furthermore, the participant should learn how password-protected compressed files can be broken; this should be covered in hands-on workshops during the training course.

Erased Files

The training participant should be shown how previously erased files can be recovered by using DOS programs and by manually using data-recovery techniques. These techniques should also be demonstrated by the participant, and cluster chaining will become familiar to the participant.

Internet Abuse Identification and Detection

The participant should be shown how to use specialized software to identify how a targeted computer has been used on the Internet. This process will focus on computer forensics issues tied to data that the computer user probably doesn't realize exists (file slack, unallocated file space, and Windows swap files).

The Boot Process and Memory Resident Programs

The participant should be able to take part in a graphic demonstration of how the operating system can be modified to change data and destroy data at the whim of the person who configured the system. Such a technique could be used to covertly capture keyboard activity from corporate executives, for example. For this reason, it is important that the participants understand these potential risks and how to identify them.

TYPES OF BUSINESS COMPUTER FORENSIC TECHNOLOGY

Finally, let's briefly look at the following types of business computer forensics technology:

- Remote monitoring of target computers
- Creating trackable electronic documents
- Theft recovery software for laptops and PCs
- Basic forensic tools and techniques
- Forensic services available

Remote Monitoring of Target Computers

Data Interception by Remote Transmission (DIRT) from Codex Data Systems (CDS), Inc. [7] is a powerful remote control monitoring tool that allows stealth monitoring of all activity on one or more target computers simultaneously from a remote command center. No physical access is necessary. Application also allows agents to remotely seize and secure digital evidence prior to physically entering suspect premises.

Creating Trackable Electronic Documents

There are so many powerful intrusion detection tools that allow the user to create trackable electronic documents that it is beyond the scope of this chapter to mention them all. See "Intrusion Detection Systems" in Chapter 3 for a detailed explanation of some of these tools.

In general, most of these tools identify (including their location) unauthorized intruders who access, download, and view these *tagged* documents. The tools also allow security personnel to trace the chain of custody and chain of command of all who possess the stolen electronic documents.

Theft Recovery Software for Laptops and PCs

If your PC or laptop is stolen, is it smart enough to tell you where it is? According to a recent FBI report, 98% of stolen computers are never recovered. According to Safeware Insurance, 1,201,000 PCs and laptops were stolen in 2002 and 2003, costing owners $7.8 billion dollars [9]. According to a recent joint Computer Security Institute/FBI survey, 72% of the Fortune 1000 companies experienced laptop theft [9].

Nationwide losses to computer component theft cost corporate America over $11 billion a year. So if your company experiences computer-related thefts and you do nothing to correct the problem, there is a 92% chance you will be hit again.

What Is the Real Cost of a Stolen Laptop or PC?

When you lose your wallet, the last thing you think of is how much it is going to cost to replace your wallet. The same is true when equipment (especially a computer) is stolen.

Our mothers always told us, an ounce of prevention is worth a pound of cure. They were right. Think about what it really costs to replace a stolen computer.

- The price of the replacement hardware.
- The price of replacing the software.
- The cost of recreating data. If possible at all, do you keep perfect back-ups?
- The cost of lost production time or instruction time.
- The loss of customer goodwill (lost faxes, delayed correspondence or billings, problems answering questions and accessing data).
- The cost of reporting and investigating the theft, filing police reports and insurance claims.
- The cost of increased insurance.

- The cost of processing and ordering replacements, cutting a check, and the like.
- If a thief is ever caught, the cost of time involved in prosecution [7].

So, doesn't it make sense to use an ounce of prevention? You don't have to be a victim.

With that in mind, SecurityKit.com has a solution: PC PhoneHome™ [9] is a software application that will track and locate a lost or stolen PC or laptop anywhere in the world. It is easy to install. It is also completely transparent to the user. If your PC PhoneHome-protected computer is lost or stolen, all you need to do is make a report to the local police. In other words, PC PhoneHome is a transparent theft protection and recovery software system that you install on your laptop or PC. Once installed, it sends an stealth email message to your address every time the computer connects to the Internet. Let's look at the following scenario [9].

PC PhoneHome Scenario

Imagine you're a small business owner and you just went out and invested several thousand dollars in the latest laptop computer, fully loaded with all the bells and whistles. On your first business trip with your new computer you leave it (you think) safely hidden in your hotel room while you entertain a client. Later that night you return to your room and your laptop, with all your work in it, has disappeared without a trace. The financial loss is bad enough, but the hours of work you've lost is worse, and the sensitivity of the information in your laptop, if it gets into the hands of the wrong people, could be a disaster [9].

Now imagine a simple, inexpensive software system that offers real hope of tracking your laptop and pinpointing its location anywhere in the world. Is this really possible or is it just another fanciful hi-tech gimmick from the imagination of the writers of the latest James Bond movie? It's no gimmick. It's PC PhoneHome, the latest in computer theft recovery software [9].

PC PhoneHome is a software application that, when installed in your laptop or desktop computer, secretly transmits an electronic message to an email address of your choice. This allows you to track and locate your computer, thus providing the potential for its ultimate recovery as well as apprehension of the thief [9].

How Does PC PhoneHome Work?

It's simple. First, you install PC PhoneHome on your computer, configuring it to send its recovery information to an email address of your choosing. PC PhoneHome sends a stealth email to your designated email address once a day, or every time you connect to the Internet and are assigned an IP address different from your previous IP address. If your computer is lost or stolen, you report the loss to the police and continue to monitor (with the additional help of the PC PhoneHome Recovery Center) your designated email address. When your stolen computer accesses the Internet by any method, your lost or stolen computer will send you its stealth email message, informing you of its location [9].

If you are a registered user of PC PhoneHome, you may seek the PC PhoneHome technical service center's assistance in locating your computer's exact coordinates and alerting the local police to recover it. As a side benefit, any other items of your property (like expensive jewelry) that might have been taken at the same time may also be recovered [9].

A success story, PC PhoneHome has been enthusiastically embraced by police forces, insurance companies, and the computer industry. The product is a natural fit for the security monitoring and Internet service provider (ISP) industry. PC PhoneHome is compatible with all Windows and Macintosh operating systems [9].

Basic Forensic Tools and Techniques

Today, many computer forensics workshops have been created to familiarize investigators and security personnel with the basic techniques and tools necessary for a successful investigation of Internet and computer-related crimes. So many workshops have been created that it is beyond the scope of this chapter to mention them all. However, throughout the book, a number of them will be mentioned in detail. Workshop topics normally include: types of computer crime, cyber law basics, tracing email to its source, digital evidence acquisition, cracking passwords, monitoring computers remotely, tracking online activity, finding and recovering hidden and deleted data, locating stolen computers, creating trackable files, identifying software pirates, and so on.

Forensic Services Available

Through computer forensic evidence acquisition services, forensic experts for companies like Capitol Digital Document Solutions [10] can provide management with a potent arsenal of digital tools at its disposal. They have the necessary software and hardware to travel to designated sites throughout the world to acquire an exact image of hard drives, tapes, etc. This image is an exact duplication of the source media and allows evaluation within their laboratories with minimal disruption to others. Services include but are not limited to

- Lost password and file recovery
- Location and retrieval of deleted and hidden files
- File and email decryption
- Email supervision and authentication
- Threatening email traced to source
- Identification of Internet activity
- Computer usage policy and supervision
- Remote PC and network monitoring

- Tracking and location of stolen electronic files
- Honeypot sting operations
- Location and identity of unauthorized software users
- Theft recovery software for laptops and PCs
- Investigative and security software creation
- Protection from hackers and viruses (see sidebar, "Virus/Trojan/Worm Protection") [10]

VIRUS/TROJAN/WORM PROTECTION

The following are tips to avoid a computer virus and trojan and worm programs:

- Don't open attachments sent with junk email or emails from persons you do not know.
- Don't open any files attached to an email if the subject line is questionable or unexpected. If you need to open the file, always save it to your hard drive before doing so.
- Disable the Windows Scripting Host. Recently, Microsoft introduced a "macro" programming language into the core of Windows and IE browsers, which allows Visual Basic scripts to run without the need for specialist software. Although this can make your computer easier to use (being able to program shortcuts, or use third-party Visual Basic scripts), it is also a security risk. A typical PC does not need Windows Scripting Host to function correctly, and it should be safe to disable it. To remove Windows Scripting Host from your computer, open up your Control Panel and select the Add/Remove Programs icon. Select the Windows Setup tab, double-click the Accessories section and untick the box next to "Windows Scripting Host."
- Always download files from well-known established and trusted sites. Always know the source of any attachment and file. Install an anti-virus program. This program will scan any file or attachment you get over the Net for known viruses. The program will warn you if any virus is detected.
- Correctly configure the anti-virus software so that it performs as designed. An improperly configured anti-virus software can be as good as no software.
- If your anti-virus program has an automatic virus scanning feature, keep this feature activated just in case you forget to scan for the virus.
- Back up your files on a regular basis. If a virus destroys your files, at least you can replace them with your backup copy. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer.

→

- Get immediate protection. Configure your anti-virus software to boot automatically on start-up and run at all times. In case you forget to boot up your anti-virus software, configuring it to start by itself will ensure you are always protected.
- Educate yourself about the latest viruses. Many Web sites keep a list of all old and new viruses.
- Write-protect all system and software diskettes using the write-protect tab to prevent any virus from spreading. Using the write-protect tab will prevent viruses from being transmitted to those sensitive or critical system disks.
- Don’t boot from a floppy disk. Floppies are a common way viruses are transmitted. If you use a floppy while working on your computer, remove it when you shut the machine off or the computer will automatically try to boot from the floppy, perhaps launching any viruses on the disk.
- Don’t share floppies. Even a well-meaning friend may unknowingly pass along a virus, trojan horse, or worm.
- Scan floppies before using them. This is always important, but especially if you are using the disk to carry information between one computer and another. You could easily pick up a virus from an insecure network and introduce it into your system. Running a virus scan before launching any of the programs on the disk will prevent infection.
- If you are in a network environment and you get infected, report the virus to your systems administrator, who can them determine the source of the infection. This will ensure that the virus will not spread.
- If you use Microsoft Outlook (not Express) for email, make sure that the Automatic preview feature is disabled. You can find this option under the View menu.
- Outlook and Outlook Express users are the most targeted. Consider using a different email program.
- If you must use one of the Outlooks, download all of Microsoft’s security patches. Add your own address to your Outlook address book, so if it starts sending out messages on its own, at least you’ll know about it.
- Keep in mind that often computer viruses are spread by accident, so files you get from a friend who would not purposely infect you still might give you a virus [12].

SPECIALIZED FORENSICS TECHNIQUES

Threats to the strategic value of your business almost always involve a computer or network because that is where your company’s proprietary information and business processes are located. A simple and virtually undetectable fraud that posts a few cents to a phony account can reap a perpetrator thousands of dollars flowing through accounts payable. A malicious change to an individual's personnel records could cost the person a job and a career. Divulging a company's financial records could damage it on Wall Street, in the marketplace, and before shareholders. Corporate espionage can steal trade secrets. Posting libelous information on the Internet about a company or individual can damage a reputation beyond recovery. Employees of a company might be stealing from it or using company resources to work for themselves, or they can be using excessive work time to surf pornographic sites and play games [11].

Computer forensics investigators examine computer hardware and software using legal procedures to obtain evidence that proves or disproves allegations. Gathering legal evidence is difficult and requires trained specialists who know computers, the rules of evidence gathering, and how to work with law enforcement authorities [11].

Computer forensics examiners should be called in when a threat to a company's business and reputation is serious. Any organization that does not have a way to detect and stop malicious behavior can be victimized with no legal recourse. Preserving evidence according to Federal Rules of Evidence gives choices that otherwise would not exist. When an intruder attacks or steals from an organization, the ability or threat to get law enforcement involved may be the only way to reduce the damage or prevent future occurrences. Gathering computer evidence is also useful for confirming or dispelling concerns about whether an illegal incident has occurred and for documenting computer and network vulnerabilities after an incident [11].

Companies employ computer forensics when there is serious risk of information being compromised, a potential loss of competitive capability, a threat of lawsuits, or potential damage to reputation and brand. Some companies regularly use forensic investigations to check employee computers. In theory, employees are less tempted to stray when they know they are being watched [11].

On the other hand, when the cost of a forensic investigation exceeds potential gain, there is little reason to use it. Companies have used legal evidence gathering to drive home points with employees and external intruders even though the cost of investigations exceeded recovery. Usually, however, a full-scale investigation is not needed to stop an inappropriate action such as surfing that wastes time. Computer forensics also may not be needed when computers and networks play a minor role in an incident or threat, but this may not always be clear. The relationship between the computer and an event under inquiry is critical, and sometimes until a forensics examination has been done, one cannot know whether a computer was a significant part of an event or not.

Legal Evidence

A computer forensics examiner always should gather and preserve evidence according to Federal Rules of Evidence. The examiner has three basic tasks: finding, preserving, and preparing evidence. Finding and isolating evidence to prove or disprove allegations is as difficult as preserving it. Investigators can plow through thousands of active files and fragments of deleted files to find just one that makes a case. Computer forensics has been described as looking for one needle in a mountain of needles. Preserving computer evidence is important because data can be destroyed easily. The 1s and 0s that make up data can be hidden and vanish instantly with a push of a button. As a result, forensics examiners assume every computer has been rigged to destroy evidence, and they proceed with care in handling computers and storage media [11].

Preparing evidence requires patience and thorough documentation so it can withstand judicial scrutiny. For example, a hacking incident at a Web music store was thrown out of court because examiners who prepared the case failed to follow rules of evidence that documented where evidence had come from and that it had not been changed [11].

Preserving computer evidence requires pre-incident planning and training of employees in incident discovery procedures. System administrators sometimes think they are helping a forensics examiner when they are actually destroying evidence. Managers should make sure that there's minimal disturbance of the computer, peripherals, and area surrounding the machine. If a computer is turned on, leave it on; if turned off, leave it off. Moreover, never run programs on a computer in question. For example, running Windows to examine files destroys evidence in the swap file. Finally, never let a suspect help open or turn on a machine [11].

Gathering computer evidence goes beyond normal data recovery. Unfortunately, there are no certified procedures for safe evidence gathering, nor is there a single approach for every type of case. Examiners work in secure laboratories where they check for viruses in suspect machines and isolate data to avoid contamination [11].

Examiners will, for example, photograph equipment in place before removing it and label wires and sockets so computers and peripherals can be reassembled exactly in a laboratory. They transport computers, peripherals, and media carefully to avoid heat damage or jostling. They never touch original computer hard disks and floppies. They make exact bit-by-bit copies and they store the copies on a medium that cannot be altered, such as a CD-ROM. When suspects attempt to destroy media, such as cutting up a floppy disk, investigators reassemble the pieces to read the data from it. Nor do examiners trust a computer's internal clock or activity logs. The internal clock might be wrong, a suspect might have tampered with logs, or the mere act of turning on the computer might change a log irrevocably [11].

Before logs disappear, investigators are trained to capture the time a document was created, the last time it was opened, and the last time it was changed. They then calibrate or recalibrate evidence based on a time standard or work around log tampering, if possible [11].

Investigators always assume the worst. It is a rule in computer forensics that only the physical level of magnetic materials where the 1s and 0s of data are recorded is real, and everything else is untrustworthy. A suspect might have corrupted all of the software operating systems, applications, and communications in a computer, or the software itself might erase evidence while operating, so forensic examiners avoid it [11].

Examiners search at the bit level of 1s and 0s across a wide range of areas inside a computer, including email, temporary files in the Windows operating system and in databases, swap fields that hold data temporarily, logical file structures, slack and free space on the hard drive, software settings, script files that perform preset activities, Web browser data caches, bookmarks, and history and session logs that record patterns of usage. They then correlate evidence to activities and sources [11].

Investigators have many tricks that help them get around the clever suspect. For example, they often do not attempt to decode encrypted files. Rather, they look for evidence in a computer that tells them what is in the encrypted file. Frequently, this evidence has been erased, but unencrypted traces remain to make a case. For data concealed within other files or buried inside the 1s and 0s of a picture, an investigator can tell the data is there even though it is inaccessible. Nearly identical files can be compared to see their minute differences [11].

When forensic examiners find computer evidence, they must present it in a logical, compelling, and persuasive manner that a jury will understand and a defense counsel cannot rebut. This requires step-by-step reconstructions of actions with documented dates and times, charts and graphs that explain what was done and how, testimony that explains simply and clearly what a suspect did or did not do, and exhibits that can withstand scrutiny [11].

Case presentation requires experience, which only can be gained through courtroom appearances. This is why lawyers and managers should retain computer forensics examiners who have a record of successful expert testimony on computer evidence. An experienced examiner knows the questions that opposing attorneys will ask and the ways to provide answers that withstand challenge. A skilled litigator can defeat an inexperienced examiner for failing to collect evidence in a proper manner and failing to show that evidence supports allegations. Not long ago, attorneys knew little about computers and how they operated, but today they do and they are increasingly skilled at challenging examiners' methods [11].

A Growing Service

With the growth of computers and networks comes the growth of crime committed through or with computers and networks. It is a fast-growing field because computers and networks have moved to the heart of business and societal operations. However, it is not a service that most corporations will or should establish internally. Because investigations are so specialized, few organizations have the human or technical resources to gather and compile evidence that withstands court challenges. Large multinational corporations have or may develop the capability, but most organizations will purchase computer forensics as needed or keep a computer forensics firm on retainer. It's important that managers and lawyers remember that computer evidence is fragile and that the best way to handle an incident is to isolate it until examiners take over [11].

HIDDEN DATA AND HOW TO FIND IT

As if you didn't have enough to worry about, today's technology presents your business with as many problems as it does solutions. Computers that work miracles in your day-to-day operations often malfunction—and you lose valuable data. The email that makes communicating so simple, carries deadly viruses that infect your machines and spread, causing massive data losses throughout your network. Hackers, both inside and outside your company, can access your information, manipulate it, hide it, steal it, and cause huge losses of data [14].

In many cases, documents and files deleted from a computer can be found and recovered using the methods of computer forensics. When files or documents are deleted from a computer, the majority of the actual information is typically left behind. Although the user may think the deleted document has been eradicated, this is usually not the case [14].

Documents and files deleted or hidden even years ago may be recovered through a computer investigation. Deleted or hidden files are one of the prime targets of the computer forensic technician searching for evidence [14].

What can you do about it right away? You should turn to computer forensic technicians or specialists (like Kessler International) for hard drive data recovery and other data recovery services [14]. These technicians specialize in professional data recovery and will restore your data quickly—right when you need it. These teams of data recovery experts know how to retrieve your lost data from damaged and corrupt storage media including hard drives, back-up systems, temporary storage units, and more. They can also restore individual corrupt files back to their original condition [14].

SPYWARE AND ADWARE

Spyware is Internet jargon for advertising supported software (adware). It is a way for shareware authors to make money from a product, other than by selling it to the users. There are several large media companies that approach shareware authors to place banner ads in their products in exchange for a portion of the revenue from banner sales. This way, you don't have to pay for the software, and the developers are still getting paid. If you find the banners annoying, there is usually an option to remove them by paying the regular licensing fee.

Why Is It Called Spyware?

While this may be a great concept, the downside is that the advertising companies also install additional tracking software on your system, which is continuously *calling home*, using your Internet connection to report statistical data to the "mothership." While according to the privacy policies of the companies, there will be no sensitive or identifying data collected from your system and you shall remain anonymous, the fact still remains that you have a *live* server sitting on your PC that is sending information about you and your surfing habits to a remote location.

Are All Adware Products Spyware?

No, but the majority are. There are also products that display advertising but do not install any tracking mechanism on your system.

Is Spyware Illegal?

Even though the name may indicate so, spyware is not an illegal type of software in any way. However, there are certain issues that a privacy-oriented user may object to and therefore prefer not to use the product. This usually involves the tracking and sending of data and statistics via a server installed on the user's PC and the use of your Internet connection in the background.

What's the Hype About?

While legitimate adware companies will disclose the nature of data that is collected and transmitted in their privacy statement (linked from their database, there is almost no way for the user to actually control what data is being sent). The technology is in theory capable of sending much more than just banner statistics and this is why many people feel uncomfortable with the idea.

On the Other Hand

Millions of people use advertising supported spyware products and could not care less about the privacy hype. In fact, some spyware programs are among the most popular downloads on the Internet.

Real Spyware

There are also many PC surveillance tools that allow a user to monitor all kinds of activity on a computer, ranging from keystroke capture, snapshots, email logging, chat logging, and just about everything else. These tools are often designed for parents, businesses, and similar environments but can be easily abused if they are installed on your computer without your knowledge. Furthermore, these tools are perfectly legal in most places, but, just like an ordinary tape recorder, if they are abused, they can seriously violate your privacy.

ENCRYPTION METHODS AND VULNERABILITIES

The use of encryption provides a different kind of challenge for the forensic investigator. Here, data recovery is only half the story, with the task of decryption providing a potentially greater obstacle to be overcome. Encryption, whether built into an application or provided by a separate software package, comes in different types and strengths.

Some of the most commonly used applications provide encryption protected by passwords that can be readily defeated by investigators with the right tools and the time to use them. Other types of encryption, readily available to the general public, can be configured and used to create encrypted data that goes beyond the ability of the professional investigator to decrypt it using software. Nevertheless, in these cases it may still be possible to decrypt data by widening the scope of the investigation to include intelligence sources beyond the computer under investigation. For example, public key encryption can be used to create highly secure, encrypted data. To decrypt data encrypted in this fashion, a private key and passphrase is needed. The private key may be found on the suspect's machine or backed up to removable media. Similarly, the passphrase may be recorded somewhere on the computer in case it is forgotten or may be written down somewhere and kept in a nearby location.

For example, three recent developments have added to the remarkable insecurity of the Net. One affects email. The other two affect network systems. First, a weakness has been discovered in the world's most popular encryption program that, in some circumstances, allows the encryption program to be completely bypassed. People using this program to encrypt email to protect its privacy and confidentiality may be thwarted despite their efforts. Second, hackers have recently discovered a cloaking program that allows them to blow past firewalls on servers and networks without being detected. Third, a flaw has been announced that affects networks around the globe regarding the file transfer protocol (FTP) used on the Internet. These three revelations taken together are seriously bad news for Internet privacy, confidentiality, and security.

The Fallacies of Encryption and Password Protection

How serious is the problem? Very. If a snoop can gain physical access to your computer or floppy disk where you store your secret key, he can modify it and wait for you to use it. When you do, he or she is secretly notified. From that point on, he has access to the rest of your encrypted personal information and you never know it. In effect, the snoop bypasses a user's *password* and bypasses the effects of encryption entirely. In this instance, the protection offered by encryption is illusory. Likewise, if a hacker can electronically break into your computer, and you have your secret key stored there, the security of your digital signature or your encrypted files is worthless.

Internet and Email Encryption and Security

For several years lawyers have been advised to use encryption programs to scramble sensitive email messages before sending them. The most popular encryption program is called PGP, or Pretty Good Privacy, invented by Phil Zimmerman a decade ago. PGP is a dual key, algorithm-based code system that makes encrypted data practically impossible to decipher. PGP is now owned by Network Associates, Inc. Of the 800 million people using the Internet, about 60 million use PGP to encrypt email.

In February 2001, Zimmerman went to work for Hushmail (an encrypted email system), aiming to make the use of PGP simpler and user friendly. His second goal was to work toward making PGP an international standard. To everyone's surprise, a month later, in March 2001, two engineers with a Czechoslovakian research group announced that they had found a serious flaw in the open PGP format.

The flaw is serious for two reasons. First, open PGP is the most widely used encryption system in the world. Until recently many systems that make e-commerce available by credit card on the Internet have been based on PGP. These products are still in use worldwide. Second, the theory behind PGP is essentially the same as that used in the Rivest, Shamir and Adleman (RSA) standard for digital signatures. The presumed *security* of this technique was what persuaded Congress to pass the Digital Signatures Act, which is based on RSA standards.

Next, let's briefly look at how to protect data from being compromised. In other words, to protect data from being compromised, experts use computer forensics.

PROTECTING DATA FROM BEING COMPROMISED

In the past 25 years, since the introduction of the personal computer, a great change has taken place in the way people use computers. No longer are they an obscure rarity, but are ubiquitous, and the business without a computer is now an exception. They are used to assist with most tasks in the workplace. You communicate via email and chat, and even voice and video communication uses computers. You maintain financial records, schedule appointments, and store significant amounts of business records, all electronically.

It should come as no surprise that with this newfound productivity comes a class of individuals who exploit these benefits to commit crimes and civil wrongs. Almost any type of investigation and litigation today may rely on protecting evidence obtained from computer systems. Digital evidence can often make or break a case. This evidence may be used to establish that a crime has been committed or assert other points of fact in a court of law, such as identify suspects, defend the innocent, prosecute the guilty, and understand individuals' motives and intents.

As previously explained, computer forensics is the science whereby experts extract data from computer media in such a way that it may be used in a court of law. In other words, computer forensics is used by experts to protect data from being compromised. This evidence may include such things as deleted emails or files and computer logs, spreadsheets, and accounting information.

It is not sufficient to merely have the technical skills to locate evidence on computer media. Computer forensics experts recover the evidence and maintain a strict chain of custody to ensure that the evidence is preserved in its original form. These experts' knowledge of what to look for and where to look is also important.

Now let's look at what has become a very popular undertaking: Internet tracing methods. How can you find out who is sending you email from a certain AOL or Hotmail account? Well, that's not what this next section is about is about. It is about how you can find out whether someone faked his or her email address and how you can find out from which account that mail really was sent [13].

INTERNET TRACING METHODS

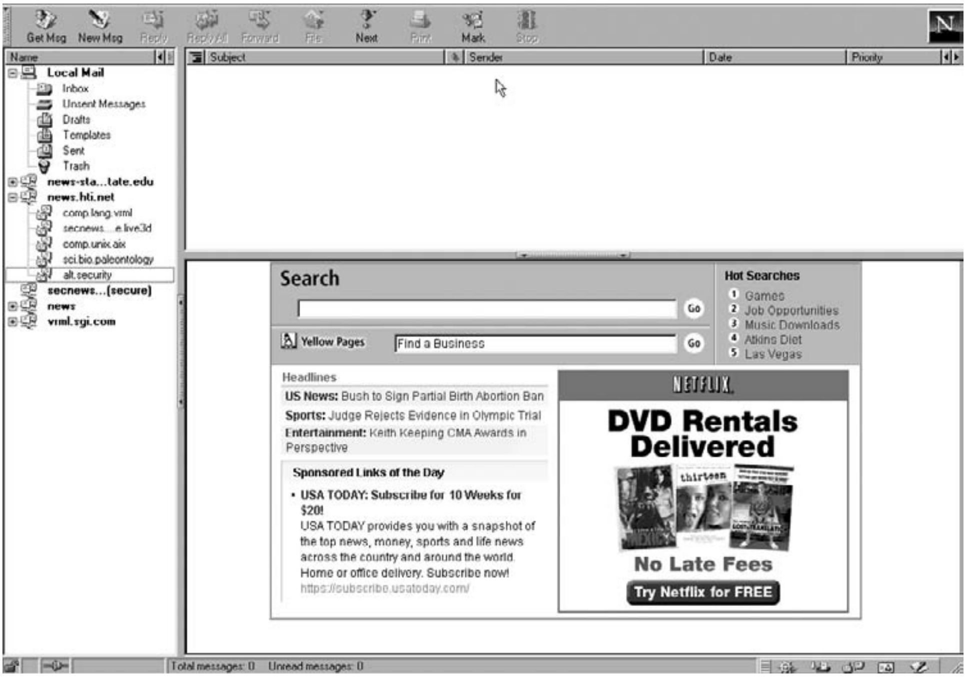
If an email comes from a real, valid email account and you want to know who the person behind that email account is, then you most likely will need to serve the Internet provider who is hosting that email account a court-order. Another idea would be to take that email address and search for it on the Web and usenet. Who knows, he might have posted somewhere with his real name and address [13].

Sometimes people might send you information or hate mail from a fake address. This can be done quite easily by simply changing the Sender and Return-to fields to something different. You can do this, since these fields (your identity), are normally not checked by the mailserver when you send mail, but only when you receive mail [13].

Every email has a so-called header. The header is the part in which the route the email has taken is being described. Since the header is rather ugly, it is normally hidden by the email program. Every email program can display them, though (look into the Options or Preferences menu) [13].

The email text lines below are a typical, but not particularly sophisticated, example of faked email. Fortunately, most people are not more sophisticated than this. You should, however, be aware that there are much more sophisticated ways to fake email. A message sent to the newsgroup alt.security (see Figure 2.2) [13] and archived (*http://catalog.com/mrm/security/trace-forgery.html*) on the Web explains one possible way to deal with some of these cases. But for now, back to the *easy cases,* as shown by the following email lines [13]:

```
Received: from SpoolDir by IFKW-2 (Mercury 1.31);
13 May 98 15:51:47 GMT +01
Return-path: <kuno@seltsam.com>
Received: from bang.jmk.su.se by ifkw-2.ifkw.uni-muenchen.de (Mercury
1.31) with ESMTP;
13 May 98 15:51:44 GMT +01
Received: from [130.237.155.60] (Lilla_Red_10 [130.237.155.60]) by
bang.jmk.su.se (8.7.6/8.6.6) with ESMTP id PAA17265 for <luege-
ti@ifkw.uni-muenchen.de>; Wed, 13 May 1998 15:49:09 +0200 (MET DST)
X-Sender: o-pabjen@130.237.155.254
Message-Id: <v03020902b17f551e91dd@[130.237.155.60]>
Mime-Version: 1.0
```



Headlines

US News: Bush to Sign Partial Birth Abortion Ban

Sports: Judge Rejects Evidence in Olympic Trial

Entertainment: Keith Keeping CMA Awards in Perspective

Sponsored Links of the Day

- **USA TODAY: Subscribe for 10 Weeks for $20!**
USA TODAY provides you with a snapshot of the top news, money, sports and life news across the country and around the world. Home or office delivery. Subscribe now!
https://subscribe.usatoday.com/

FIGURE 2.2 A message sent to the newsgroup alt.security.

```
Content-Type: text/plain; charset=”us-ascii”
Date: Wed, 13 May 1998 15:49:06 +0200
To: luege-ti@ifkw.uni-muenchen.de
From: Kuno Seltsam <kuno@seltsam.com>
Subject: Important Information
X-PMFLAGS: 34078848 0
```

Now let’s go through the email line by line [13]:

```
Date: Wed, 13 May 1998 15:49:06 +0200
To: luege-ti@ifkw.uni-muenchen.de
From: Kuno Seltsam <kuno@seltsam.com>
Subject: Important Information
```

The preceding lines should look quite familiar. They describe who claims to have sent the mail, to whom it was sent, and when. The following line is a number that your email program (in this case Pegasus Mail) might add to the mail to keep track of it on your hard disk [13]:

```
X-PMFLAGS: 34078848 0
```

The following lines state that the message contains normal, plain text without any *fancy* letters like umlauts, etc. [13]:

```
Mime-Version: 1.0 Content-Type: text/plain;
charset=”us-ascii”
```

The following line contains a tracking number, which the originating host has assigned to the message. The Message-Id is unique for each message and in this case contains the IP number of the originating host. If you for some reason doubt that the message really came from someone at *seltsam.com*, you can now take this number and have it translated into something more meaningful. For this task, you can, for example, use TJPing (*http://www.topjimmysoftware.com/*), a small program that tracks IP packages online and resolves IP numbers [13]:

```
Message-Id: <v03020902b17f551e91dd@[130.237.155.60]>
```

If you use TJPing, the real name of the originating computer is [13]:

```
Starting lookup on 130.237.155.60 - May 14, 1998
22:01:25
Official Name: L-Red-10.jmk.su.se
IP address: 130.237.155.60
```

This is the originating computer from which the message was sent, not the mailserver. If the address was at a university, as in this case, this is not a great help, since there are many students using the same computers all day. The situation is very different within companies, though, since employees tend to have their own computers, which no one else uses. If the header doesn't show any further information, you might use this information by calling the company's system administration and ask, "Say, who's sitting at Node 60?" Amazingly, often you will get a reply. It is comparatively easy to find out which company you are dealing with. Just cut off the first set of digits from the Official Name (L-Red_10.), add www and type it into your browser. You will see that *www.jmk.su.se* is the journalism department of the University of Stockholm [13].

The following line is solid gold. This tells you who was logged on to the mailserver when the message was sent. Not all email programs add this line, though. Eudora (*http://www.eudora.com/*) does, whereas Pegasus Mail doesn't [13].

```
X-Sender: o-pabjen@130.237.155.254
```

So now you know that the user who sent us the mail is o-pabjen. The IP number is that of the mailserver used (checking with TJPing [*http://www.topjimmysoftware.com/*], you learn that it's called bang.jmk.su.se). Now you could actually reply to the message by sending a mail to o-pabjen@130.237.155.254 or o-pabjen@bang.jmk.su.se [13].

Maybe you want to know his or her real name. In this case, you can try to *Finger* the account. Finger is a command that reveals basic information about the account holder. Due to the increased attention to privacy online, more and more servers have disabled it. It is always worth a try, though. Using WSfinger (*http://www.etoracing.com/wsfinger.htm*), you'll learn the following [13]:

```
Login name: o-pabjen In real life: Pabst Jens global
```

So, now you have a name: Jens Pabst. *Global* could be part of the name or be some kind of code added by the system administration for internal purposes.

If you manage to obtain the information that's been accumulated so far, then you don't actually have to look any further. You have what you want. "Kuno Seltsam <kuno@seltsam.com>" is really Jens Pabst <o-pabjen@bang.jmk.su.se>. But, let's go through the rest of the header anyway [13]:

```
Received: from [130.237.155.60] (Lilla_Red_10 [130.237.155.60]) by
bang.jmk.su.se (8.7.6/8.6.6) with ESMTP id PAA17265 for <luege-
ti@ifkw.uni-muenchen.de>; Wed, 13 May 1998 15:49:09 +0200 (MET DST)
```

The preceding lines state which computer the mailserver has received the message from, when, and that the message is supposed to be sent to luege-ti@ifkw.uni-muenchen.de.

Similar to the last part of the header, the following lines tell you from where the recipient's mailserver (ifkw-2.ifkw.uni-muenchen.de) has received the message. You know that this must be the recipient's mailserver, since it is the last server that receives anything [13].

```
Received: from bang.jmk.su.se by ifkw-2.ifkw.uni-muenchen.de (Mercury
1.31) with ESMTP; 13 May 98 15:51:44 GMT +01
```

It follows the fake return path:

```
Return-path: <kuno@seltsam.com>
```

and an internal message from the mailserver about where and how it distributed the message within its system. You know that "SpoolDir" cannot be the recipient's mailserver, since it lacks an Internet address (something like server.somewhere.de) [13].

```
Received: from SpoolDir by IFKW-2 (Mercury 1.31); 13 May 98 15:51:47
GMT +01
```

This next section is intended to familiarize the computer forensic investigator with various methodologies and tools available to perform a forensic examination of a Research In Motion (RIM) wireless (BlackBerry) device. The procedures and tools presented here are by no means all encompassing but are intended to elicit design of custom tools by those more programmatically inclined. The methods have been tested using an Exchange Edition RIM pager and an Exchange Edition RIM handheld.

SECURITY AND WIRELESS TECHNOLOGIES

There are two types of RIM devices within each model class. The Exchange Edition is meant for use in a corporate environment, while the Internet Edition works with standard POP email accounts. The Exchange Edition employs Triple-DES encryption to send and receive, but the Internet Edition communicates in clear text. Neither employs an encrypted files system.

Relevance of RIM Computer Forensics

A RIM device shares the same evidentiary value as any other personal digital assistant (PDA). As the computer forensics investigator may suspect of most file systems, a delete is by no means a total removal of data on the device. However, the RIM's always-on, wireless push technology adds a unique dimension to forensic examination. Changing and updating data no longer requires a desktop synchronization. In fact, a RIM device does not need a cradle or desktop connection to be useful. The more time a PDA spends with its owner, the greater the chance is that it will more accurately reflect and tell a story about that person. Thus, the RIM's currently unsurpassed portability is the examiner's greatest ally.

Evidence Collection: Gathering Logs

The first procedure of evidence collection violates the computer forensic method by requiring the investigator to record logs kept on the unit that will be wiped after an image is taken. The logs must be accessed on the original unit before the programmer software development kit (SDK) tool is applied. The logs are not accessed via the standard user interface. Rather, they are reviewed using the following hidden control functions.

Imaging and Profiling

An image should be taken of the file system as the very first step as long as the logs are not required or a method of extracting the logs from the image is developed. An image or bit-by-bit backup is acquired using an SDK utility that dumps the contents of the Flash RAM into a file easily examined with a hex editor. The Program Loader, which is used to perform most of the inspection in addition to taking the image, will cause a reset each time it is run. A reset can mean a file system cleanup. This means that to get a partition table, you risk changing the file system and spoiling the data.

Evidence Review

Two options are available for information review using the hex dump: manual review of the Hex file using a hex editor and loading of the hex file into the BlackBerry SDK simulator for review. The hex editor will provide access to the entire file system including deleted or *dirty* records indicated by byte 3 of the file header. Using the SDK will assist in *decoding* dates on extant records.

The File System

The RIM file system is abstracted to appear as a database to most available Application Programming Interfaces (APIs) in order to simplify programming. This abstraction qualifies as a file translation layer (FTL), hiding what is really a quite complicated system of file management. Under the hood of your RIM device is a standard Flash RAM used to store all nonvolatile data.

Flash is organized similarly to *dynamic random access memory* (DRAM) and has the 65 ns read performance to match. However, write performance is slower by a factor of nearly 1000 times. Writing flash is a binary AND or NAND, meaning each 1 in memory can be toggled to 0 but not back again without an erasure. However, an erasure can only occur in blocks of 64 KB, while writing can occur in any interval. An erasure costs more in terms of time than a write because of conditioning. Conditioning means forcing every 1 to a 0 before resetting (erasing) all bits to 1 again in order to prolong the life of the Flash RAM

Data Hiding

Data hiding is accomplished in several ways on a RIM device. Hidden databases, partition gaps, and obfuscated data are but a few. Presented here are a few ideas to get the computer forensics investigator thinking in the right direction.

Custom databases with no icon in the Ribbon graphical user interface (GUI) are capable of providing hidden data transport. A hacker may write a program that utilizes a database accessible only through device synchronization. The average user or uninformed investigator will never have knowledge of the *hidden* database. For example, a database reader can thwart such an attempt, as it will provide access to all databases on a unit. Unfortunately, it will need to be installed on the unit investigated for it to function.

Now let's look at what the computer forensics specialist sees in firewall logs, especially what port numbers mean. The computer forensics specialist can use this information to help figure out what hackers or worms are up to.

AVOIDING PITFALLS WITH FIREWALLS

All the traffic going through a firewall is part of a connection. A connection consists of the pair of IP addresses that are talking to each other, as well a pair of port numbers that identify the protocol or service. The destination port number of the first packet often indicates the type of service being connected to. When a firewall blocks a connection, it will save the destination port number to its logfile. This section describes some of the meanings of these port numbers as well as avoiding some of the pitfalls. Port numbers are divided into three ranges:

- The well-known ports are those from 0 through 1023. These are tightly bound to services, and usually traffic on this port clearly indicates the protocol for that service. For example, port 80 virtually always indicates HTTP traffic.
- The registered ports are those from 1024 through 49151. These are loosely bound to services, which means that while there are numerous services

"bound" to these ports, these ports are likewise used for many other purposes that have nothing to do with the official server.

- The dynamic and private ports are those from 49152 through 65535. In theory, no service should be assigned to these ports.

In reality, machines start assigning *dynamic* ports starting at 1024. However, there are exceptions: for example, Sun starts their RPC ports at 32768.

Suppose you are seeing attempts on the same set of ports from widely varying sources all over the Internet. Usually, this is due to a "decoy" scan, such as in "nmap." One of them is the attacker; the others are not.

Computer forensics and protocol analysis can be used to track down who this is. For example, if you ping each of the systems, you can match up the time to live (TTL) fields in those responses with the connection attempts. This will at least point a finger at a decoy scan. The TTLs should match; if not, then they are being spoofed. Newer versions of scanners now randomize the attacker's own TTL, making it harder to weed them out.

You can also attempt to go back further in your logs, looking for all the decoy addresses or people from the same subnets. You will often see that the attacker has actually connected to you recently, while the decoyed addresses haven't. A detailed discussion of firewall pitfalls comes up in Chapter 3.

Now let's briefly look at how both government and commercial organizations are implementing secure biometric personal identification (ID) systems to improve confidence in verifying the identity of individuals seeking access to physical or virtual locations for computer forensics purposes. In other words, a secure biometric personal ID system is designed to solve the fundamental problem of verifying that individuals are who they claim to be.

BIOMETRIC SECURITY SYSTEMS

The verification of individuals for computer forensics purposes is achieved using a recognized ID credential issued from a secure and effective identity confirmation process. A secure personal ID system design will include a complex set of decisions to select and put in place the appropriate policies and procedures, architecture, technology, and staff to deliver the desired level of security. A secure biometric ID system can provide individuals with trusted credentials for a wide range of applications-from enabling access to facilities or secure networks, to proving an individual's rights to services, to conducting online transactions.

With the preceding in mind, biometric security systems for computer forensics purposes are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics.

Biometric technologies, when used with a well-designed ID system, can provide the means to ensure that an individual presenting a secure ID credential has the absolute right to use that credential. Smart cards have the unique ability to store large amounts of biometric and other *data,* carry out their own on-card functions, and interact intelligently with a smart card reader. Secure ID systems that require the highest degree of security and privacy are increasingly implementing both smart card and biometric technology.

Finally, in an ID system that combines smart card and biometric technologies for computer forensics proposes to verify the identity of individuals, a "live" biometric image (scan of a fingerprint or hand geometry) is captured at the point of interaction and compared to a stored biometric image that was captured when the individual enrolled in the ID system. Smart cards provide the secure, convenient, and cost-effective ID technology that stores the enrolled biometric template and compares it to the live biometric template. A secure ID system using smart card and biometric technology provides:

- Enhanced privacy, securing information on the card, allowing the individual to control access to that information, and removing the need for central database access during identity verification
- Improved security, protecting information and processes within the ID system and actively authenticating the trust level of the environment before releasing information
- Improved ID system performance and availability through local information processing and contactless ID card and reader implementations
- Improved system return on investment through the flexibility and upgradability that smart cards provide, allowing support of different authentication methods and multiple, evolving applications [15]

SUMMARY

Since the invention of the personal computer in 1981, new computer technologies have provided unintended benefits to criminals in the commission of both traditional crimes and computer crimes. Today computers are used in every facet of life to create messages, compute profits, transfer funds, access bank accounts, and browse the Internet for good and bad purposes. Notebook computers provide computer users with the benefits of portability as well as remote access to computer networks. Computer users today have the benefits of super computer speeds and fast Internet communications on a worldwide basis. Computers have increased productivity in business, but they also increase the likelihood of company policy abuses, government security breaches, and criminal activity.

In the past, documentary evidence was primarily limited to paper documents. Copies were made with carbon paper or through the use of a photocopy machine. Most documents today are stored on computer hard disk drives, floppy diskettes, zip disks, and other types of removable computer storage media. This is where potential computer evidence may reside, and it is up to the computer forensics specialist to find it using sophisticated computer forensics tools and computer-evidence-processing methodologies. Paper documents are no longer considered the best evidence.

Computer evidence is unique when compared with other forms of documentary evidence. Unlike paper documentation, computer evidence is fragile, and a copy of a document stored in a computer file is identical to the original. The legal "best evidence" rules change when it comes to the processing of computer evidence. Another unique aspect of computer evidence is the potential for unauthorized copies to be made of important computer files without leaving behind a trace that the copy was made. This situation creates problems concerning the investigation of the theft of trade secrets (client lists, research materials, computer-aided design files, formulas, and proprietary software).

Industrial espionage is alive and well in the cyber age, and the computer forensics specialist relies on computer evidence to prove the theft of trade secrets. Sometimes the unauthorized copying of proprietary files can also be documented through the analysis of ambient computer data. The existence of this type of computer evidence is typically not known to the computer user, and the element of surprise can provide the computer forensics investigator with the advantage in the interview of suspects in such cases. Because of the unique features associated with computer evidence, special knowledge is required by the computer forensics specialist and the lawyers, who may rely on the computer evidence to support their position in civil or criminal litigation.

Computer evidence is relied on more and more in criminal and civil litigation actions. It was computer evidence that helped identify the now infamous blue dress in the Clinton impeachment hearings. Oliver North got into some of his trouble with the U.S. Congress when erased computer files were recovered as computer evidence. Computer evidence is also used to identify Internet account abuses. In the past, much wasted government and company staff time was attributed to the playing of the *Windows Solitaire* game on company time. Thanks to the popularity of the Internet, *Windows Solitaire* has taken a backseat to employees' unauthorized Internet browsing of pornography Web sites. Internet access by employees has also created new problems associated with employees operating side businesses through the unauthorized use of company and government Internet accounts. These types of problems are becoming more frequent as more businesses and government agencies provide employees with Internet accounts. Computer forensics tools and methodologies are used to identify and document computer evidence associated with these types of computer abuses and activities.

Computer evidence is unique in other ways as well. Most individuals think that computer evidence is limited to data stored only in computer files. Most of the relevant computer evidence is found in unusual locations that are usually unknown to the computer users. Computer evidence can exist in many forms. On Microsoft Windows and Windows NT-based computer systems, large quantities of evidence can be found in the Windows swap file. In Windows NT-based computer systems, the files are called *Page Files* and the file is named PAGEFILE.SYS by the operating system.

Computer evidence can also be found in file slack and in unallocated file space. These unique forms of computer data fall into a category of data called ambient computer data. As much as 50% of the computer hard disk drive may contain such data types in the form of email fragments, word processing fragments, directory tree snapshots, and potentially almost anything that has occurred in past work sessions on the subject computer. Ambient computer data can be a valuable source of computer evidence because of the potentially large volume of data involved and because of the transparent nature of its creation to the computer user.

Timelines of computer usage and file accesses can be valuable sources of computer evidence. The times and dates when files were created, last accessed, or modified can make or break a case.

Now let's look at some of the more common conclusions that computer forensics technology can hope to answer. The following conclusions are not exhaustive, nor is the order significant.

Conclusions Drawn

- The term *computer forensics* was coined in 1991 in the first training session held by the International Association of Computer Specialists (IACIS) in Portland, Oregon. Since then, computer forensics has become a popular topic in computer security circles and in the legal community.
- Like any other forensic science, computer forensics deals with the application of law to a science. In this case, the science involved is computer science, and some refer to it as forensic computer science.
- Computer forensics has also been described as the autopsy of a computer hard disk drive because specialized software tools and techniques are required to analyze the various levels at which computer data is stored after the fact.
- Computer forensics deals with the preservation, identification, extraction, and documentation of computer evidence. The field is relatively new to the private sector but it has been the mainstay of technology-related investigations and intelligence gathering in law enforcement and military agencies since the mid-1980s.

- Like any other forensic science, computer forensics involves the use of sophisticated technology tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing.
- Typically, computer forensic tools exist in the form of computer software.
- Computer forensics specialists guarantee accuracy of evidence processing results through the use of time-tested evidence-processing procedures and through the use of multiple software tools developed by separate and independent developers.
- The use of different tools that have been developed independently to validate results is important to avoid inaccuracies introduced by potential software design flaws and software bugs.
- It is a serious mistake for computer forensics specialists to put all of their eggs in one basket by using just one tool to preserve, identify, extract, and validate the computer evidence.
- Cross-validation through the use of multiple tools and techniques is standard in all forensic sciences. When this procedure is not used, it creates advantages for defense lawyers who may challenge the accuracy of the software tool used and, thus, the integrity of the results.
- Validation through the use of multiple software tools, computer specialists, and procedures eliminates the potential for the destruction of forensic evidence.
- The introduction of the personal computer in 1981 and the resulting popularity came with a mixed blessing.
- Society in general benefited, but so did criminals who use personal computers in the commission of crimes.
- Today, personal computers are used in every facet of society to create and share messages, compute financial results, transfer funds, purchase stocks, make airline reservations, access bank accounts, and access a wealth of worldwide information on essentially any topic.
- Computer forensics is used to identify evidence when personal computers are used in the commission of crimes or in the abuse of company policies.
- Computer forensic tools and procedures are also used to identify computer security weaknesses and the leakage of sensitive computer data.
- In the past, documentary evidence was typically stored on paper and copies were made with carbon paper or photocopy machines.
- Most documents are now stored on computer hard disk drives, floppy diskettes, zip disks, and other forms of removable computer storage media.
- Computer forensics deals with finding, extracting, and documenting this form of electronic documentary evidence.

An Agenda for Action

When completing the Forensics Technology Types Checklist (Table F2.1 in Appendix F), the computer forensics specialist should adhere to the provisional list of actions for some of the principle types of computer forensic technology. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these technologies have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and an optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Processing procedures and methodologies should not conform to federal computer evidence processing standards.
2. True or False? Computer evidence is fragile and susceptible to alteration or erasure by any number of occurrences.
3. True or False? The need to preserve the computer evidence before processing a computer should not be clearly demonstrated by the computer forensic instructor through the use of programs designed to destroy data and modify the operating systems.
4. True or False? The documentation of forensic processing methodologies and findings is not important.
5. True or False? The occurrence of random memory dumps in hidden storage areas should be discussed and covered in detail during workshops.

Multiple Choice

1. The following are what it really costs to replace a stolen computer, except:
   A. The price of the replacement hardware
   B. The price of replacing the software
   C. The cost of creating data
   D. The cost of lost production time or instruction time
   E. The loss of customer goodwill (lost faxes, delayed correspondence or billings, problems answering questions and accessing data)

2. Forensic services include but are not limited to the following, except:
   - A. Lost password and file recovery
   - B. Location and retrieval of deleted and hidden files
   - C. File and email decryption
   - D. Email non-supervision and non-authentication
   - E. Threatening email traced to source

3. Port numbers are divided into three ranges, except for two of the following:
   - A. The well-known ports are those from 0 through 2134. These are loosely bound to services, and usually traffic on this port clearly indicates the protocol for that service. For example, port 80 virtually always indicates HTTP traffic.
   - B. The well-known ports are those from 0 through 1023. These are tightly bound to services, and usually traffic on this port clearly indicates the protocol for that service. For example, port 80 virtually always indicates HTTP traffic.
   - C. The registered ports are those from 1024 through 49151. These are loosely bound to services, which means that while there are numerous services "bound" to these ports, these ports are likewise used for many other purposes that have nothing to do with the official server.
   - D. The dynamic and private ports are those from 49152 through 65535. In theory, no service should be assigned to these ports.
   - E. The registered ports are those from 1024 through 76646. These are tightly bound to services, which means that while there are numerous services "bound" to these ports, these ports are likewise used for many other purposes that have nothing to do with the official server.

4. A secure ID system using smart card and biometric technology provides the following, except:
   - A. Enhanced privacy, securing information on the card, allowing the individual to control access to that information, and removing the need for central database access during identity verification
   - B. Improved security, protecting information, and processes within the ID system and actively authenticating the trust level of the environment before releasing information
   - C. Improved ID system performance and availability through local information processing and contactless ID card and reader implementations
   - D. Improved system return on investment through the flexibility and upgradability that smart cards provide, allowing support of different authentication methods and multiple, evolving applications

E. Improved ID system return on investment through the unflexibility and gradability that smart cards do not provide, thus allowing no support of similar authentication methods and multiple, revolving applications

5. The legal aspects of a computer forensics investigation center primarily on the following two main issues:

A. The requirements that need to be met in order for evidence to be successfully presented in court and, of course, not considered legally admissible

B. The requirements that need to be met in order for evidence to be successfully presented in court and, of course, considered legally admissible

C. The right of the investigator to avoid the possibility of not incurring legal action against himself or the organization for whom he is conducting the investigation

D. The acceptance of the investigator to avoid the possibility of incurring legal action against himself or the organization for whom he is reviewing the investigation

E. The need for the investigator to avoid the possibility of incurring legal action against himself or the organization for whom he is conducting the investigation

Exercise

An accounting company needed to review approximately 10 million pages of client internal documents in the context of an audit. The data resided in email, text documents, and file attachments. The original plan was to deploy a team of professionals at the client site for a three-month document review. How would your advanced document management services center (DMSC) handle this document review?

HANDS-ON PROJECTS

A large real estate corporation retained an accounting firm to investigate allegations of embezzlement. An employee was suspected of manipulating an online accounting system to divert funds from the corporation's accounts payable section. How would the accounting firm's computer forensics team go about investigating this case?

Case Project

Let's look at a real-world scenario and see how computer forensics plays into it. It's a security person's worst nightmare. You've just inherited a large, diverse enterprise with relatively few security controls when something happens. You try to detect malicious activity at the perimeter of the network by monitoring your intrusion detection systems and watching attackers bang futilely on your firewall. Even those attackers tricky enough to slip through the firewall bounce harmlessly off your highly secured servers and trip alarms throughout the network as they attempt to compromise it. Reality is usually somewhat different: most people simply don't have the tools, or at least do not have expensive, dedicated tools. You do have ways to stop the pain.

Although 2005 has been a relatively quiet year for network compromises, there have been quite a few new attacks released and a fairly significant number of incidents as a result. For the purposes of this discussion, a number of these incidents have been blended together to create a hypothetical company, Webfile.com, to demonstrate some of the techniques we have used this year in combating intrusions.

This case project discusses forensics in a Windows environment. It will offer a brief overview of the detection and analysis of an attack incident. How would you, as a computer forensics specialist, go about detecting potential incidents, identifying the attack, and conducting host-based forensics?

Optional Team Case Project

This optional team case project discusses forensics in a Windows environment. It deals with determining the scope of the compromise and understanding what the attacker is trying to accomplish at the network level. Along the way, there will be a discussion of some of the tools and techniques that are useful in this type of detective work.

As a computer forensics specialist, you have discovered the compromise (although you have yet to identify the compromise method), identified the post-attack "fingerprint" of this particular group, and begun to understand what was happening in the enterprise. Before you start with the eradication phase of your incident response, you really need to complete the identification phase: you have yet to identify the initial compromise method or to identify the scope of the compromise!

At this point in the investigation, you have reason to believe the attackers are making illicit use of the victim network to serve content to their friends and neighbors. While it is possible that any individual content provider might not mind serving some of this material (the kind that isn't unlawful anyway), your victim network isn't getting paid for this service, and the attackers have a free ride. Of more concern, the investigation so far has yielded information that indicates the attackers have compromised both local and domain administrator accounts in your enterprise.

Your objectives are simple. You want to determine how widespread the attacker's control over the network is, what the initial compromise method was, and who the attacker is (if possible). Please explain your solution in detail.

REFERENCES

[1] Feldman, John, and Giordano, Joseph V., "Cyber Forensics," Air Force Research Laboratory's Information Directorate, Associated Business Publications, 317 Madison Ave., New York, NY 10017-5391, 2001

[2] WetStone Technologies, Inc., 273 Ringwood Rd., Freeville, NY 13068, 2001.

[3] "SafeBack 3.0 Evidence Grade Bitstream Backup Utility," New Technologies, Inc., 2075 NE Division St., Gresham, Oregon 97030. (© 2002, New Technologies, Inc. All rights reserved), 2004.

[4] "AnaDisk Diskette Analysis Tool," New Technologies, Inc., 2075 NE Division St., Gresham, Oregon, 2004. (© 2002. New Technologies, Inc. All rights reserved), 2004.

[5] "Text Search Plus," New Technologies, Inc., 2075 NE Division St., Gresham, Oregon 97030, 2001. (© 2004, New Technologies, Inc. All rights reserved), 2004.

[6] "FILTER_G: English Grammer Forensic Filter," New Technologies, Inc., 2075 NE Division St., Gresham, Oregon. (© 2004, New Technologies, Inc. All rights reserved), 2004.

[7] Codex Data Systems, Inc., 143 Main Street, Nanuet, NY 10954, 2001.

[8] "CopyQM Plus: Diskette Duplication Software," New Technologies, Inc., 2075 NE Division St., Gresham, Oregon 97030, 2001. (© 2004, New Technologies, Inc. All rights reserved), 2004.

[9] "PC PhoneHome™" is a trademark of Brigadoon Software, 143 Main St., Nanuet, New York. (PC PhoneHome Web site content: Copyright 2001-2005 Brigadoon Software, Inc. All rights reserved.) (Web site copy Copyright 2000-2005 SecurityKit.com. All rights reserved.)

[10] Capitol Digital Document Solutions, 555 Capitol Mall, Suite 540, Sacramento, California 95814, 2004.

[11] Walker, Don, "Computer Forensics: Techniques for Catching the 'Perp' Protect Company Data," Enterprise Networks & Servers, Publications & Communications, Inc. (PCI), 11675 Jollyville Rd., Suite 150, Austin, TX 78759, (© 2003-2004 by Publications & Communications Inc. [PCI]), 2004.

[12] "Data Recovery," Kessler International World Headquarters, 45 Rockefeller Plaza, Suite 2000, New York, NY 10111-2000, (© 1995-2004 Michael G. Kessler & Associates Ltd. All Rights Reserved), 2004.

[13] Luege, Timo, "Tracing Email," USUS, Baaderstr. 29, Munich, Germany 80469, (© 1998-2004 USUS], 2004.

[14] "Tips to Avoid a Computer Virus," TeCrime International, Inc., 683 N Main St., Oshkosh, Wisconsin, 2004.

[15] "Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems," Smart Card Alliance, 191 Clarksville Rd., Princeton Junction, NJ 08550, 2002.

[16] "2003 Computer Crime and Security Survey," Federal Bureau of Investigation, J. Edgar Hoover Building, 935 Pennsylvania Ave., NW, Washington, D.C. 20535-0001, 2003.

3 Types of Computer Forensics Systems

Computer forensics has become a buzz word in today's world of increased concern for security. It seems that any product that can remotely be tied to network or computer security is quickly labeled as a "forensics" system. This phenomenon makes designing clear incident response plans and corporate security plans that support computer forensics difficult. Today's corporate climate of increased competition, cutbacks and layoffs, and outsourcing makes it essential that corporate security policy and practices support the inevitability of future litigation. This chapter is intended to raise awareness of the different types of computer forensics systems and to identify crucial questions for corporate planning in support of computer forensics. Answering the questions raised in this chapter will assist managers in creating sound corporate security policies and practices that support the following computer forensics systems:

- Internet security systems
- Intrusion detection systems
- Firewall security systems
- Storage area network security systems
- Network disaster recovery systems
- Public key infrastructure security systems
- Wireless network security systems
- Satellite encryption security systems
- Instant messaging (IM) security systems
- Net privacy systems
- Identity management security systems
- Identity theft prevention systems

- Biometric security systems
- Homeland security systems

INTERNET SECURITY SYSTEMS

Internet and network security are topics that many executives and managers avoid talking about. Many feel that discussing their security implementations and policies will cause their companies to become vulnerable to attack. This lack of dialog has resulted in some executives not being fully aware of the many advances and innovations in security technology that enable companies to confidently take full advantage of the benefits and capabilities of the Internet and intranets [1].

Ironically, Internet security can provide a more secure solution, as well as one that is faster and less expensive than traditional solutions to security problems of employees photocopying proprietary information, faxing or mailing purchase orders, or placing orders by phone. The purpose of this section is to demystify and inform the executive how Internet security can easily and effectively be implemented in order to conduct computer forensics [1].

General Internet Security Principles and Architecture

The first step in defining a corporate Internet security policy is to draft a high-level management policy statement establishing a framework and context for security within an organization. This policy needs to define the adequate and appropriate Internet security measures necessary to safeguard a company's systems, networks, transactions, and data [1].

The next step is to start a systematic analysis of the assets of an organization, determining the value of information, or the possible damage to reputation should it be disclosed, along with possible risks. This step is no more difficult than the risk management that a corporation already exercises every day. Most businesses already have clearly established what information is valuable, who should have access to it, and who has responsibility for protecting it, as the Internet security hierarchy in Figure 3.1 illustrates [1].

Security Hierarchy

Information such as trade secrets, vault and authorization codes, and lock and key information are clearly of a mission critical nature, and their unintended disclosure could cause severe loss to a business or operation. In addition to Internet security,

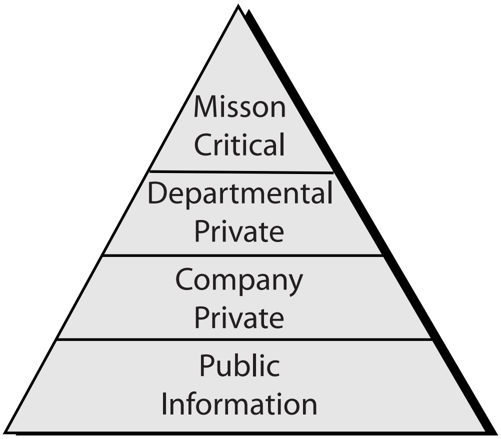


FIGURE 3.1 Internet security hierarchy.

attention should be given to physical security (restricting the use of modems and removable media and controlling access to devices) [1].

Departmental information is typically data that is private to a particular department, such as payroll information in finance and medical records in personnel. There may be legal requirements for securing this information [1].

Company private information varies from company to company but typically consists of information that should only be disclosed to employees and partners of a company, such as policy and procedure manuals. Of course, it's possible to get a bit carried away with what information is considered to be private [1].

Public information is information such as product literature, brochures, and catalogs that needs to be freely available to anyone, but whose integrity needs to be assured to prevent unauthorized alteration. This information is often provided to customers and interested parties by means of the Internet [1].

A careful and systematic examination of risks is needed, since perceptions often differ substantially from actual risks. Often the primary risk is found to be internal. For example, system administrators often are among the lowest paid individuals in an organization, yet they have access to sensitive information otherwise limited to executives. In other cases, a remote dial-in line used for debugging could be used to gain general access to internal systems, bypassing other Internet security safeguards. Care needs to be taken to rationally evaluate risk. It is often helpful to examine how existing situations are handled [1].

Implementing an Internet security policy has its price. The more security desired, the greater the cost required to provide it. Similarly, care needs to be taken to ensure that the added security does not unduly reduce network performance or employee productivity, or there will be considerable temptation to bypass or defeat corporate security measures. Thus, establishing a corporate Internet security policy involves the following:

- High-level management policy statement
- Systematic analysis of organizations assets
- Examination of risks
- Develop implementation strategy [1]

Public and Private Key Encryption

For many business and electronic commerce applications, it is necessary to transmit information over communications lines and networks where there is the potential for data to be altered, forged, or illicitly introduced. A powerful technique for securely sending information is public key encryption or public key infrastructure (which will be covered in detail later in the chapter). Two keys exist, one public, the other private. The public key is freely distributed and is used to encrypt the information to be sent. The private key is retained by the recipient and is used to decrypt the received information. Messages encrypted using long bit-length keys are currently regarded as essentially impossible to crack [1].

To use public key encryption across the Internet, steps must be taken to ensure the integrity of the public key and the identity of its owner. A trusted third party, called a "certificate authority," provides an unique "digital signature" for the public key, which cannot be forged, and both identifies the owner of the key and certifies that the key has not been altered [1].

To achieve secure, two-way communication across the Internet, without having previously exchanged keys, the Diffie-Hellman scheme may be used as shown in Figure 3.2 [1]. Each party obtains the public key for the other from a certificate authority and performs a special calculation with their own private keys. The result of the algorithm will be the same for both parties and may be used as the new secret shared key for secure communications between the two parties [1].

Network Security

Firewalls are a basic means for providing network security (and will be covered in greater detail later in this chapter). They act like the moat around a medieval castle, by restricting information to enter and leave at carefully controlled points and preventing unacceptable attempts at accessing resources within the firewall. While an important use of firewalls is to enable secure Internet access to corporate networks, they are also used to restrict access to departmental private and mission critical information [1].

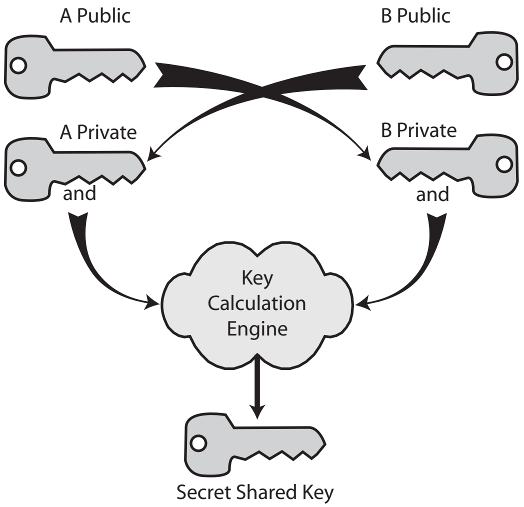


FIGURE 3.2 Diffie-Hellman calculation.

Secure Payment Solutions

Purchasing online may seem to be quick and easy, but most consumers give little thought to the process that appears to work instantaneously. For it to work correctly, merchants must connect to a network of banks (both acquiring and issuing banks), processors, and other financial institutions so that payment information provided by the customer can be routed securely and reliably. The solution is a payment gateway that connects your online store to these institutions and processors. Because payment information is highly sensitive, trust and confidence are essential elements of any payment transaction. This means the gateway should be provided by a company with in-depth experience in payment processing and security.

The Payment Processing Network

Here's a breakdown of the participants and elements involved in processing payments:

Acquiring Bank: In the online payment processing world, an acquiring bank provides internet merchant accounts. A merchant must open an internet merchant account with an acquiring bank to enable online credit card authorization and payment processing. Examples of acquiring banks include Merchant eSolutions and most major banks.

Authorization: The process by which it is verified that a customer's credit card is active and they have the credit available to make a transaction. In the online payment processing world, an authorization also verifies that the billing information the customer has provided matches up with the information on record with their credit card company.

Credit Card Association: A financial institution that provides credit card services that are branded and distributed by customer issuing banks. Examples include Visa® and MasterCard®.

Customer: The holder of the payment instrument—such as credit card, debit card, or electronic check.

Customer Issuing Bank: A financial institution that provides a customer with a credit card or other payment instrument. Examples include Citibank and Suntrust. During a purchase, the customer issuing bank verifies that the payment information submitted to the merchant is valid and that the customer has the funds or credit limit to make the proposed purchase.

Internet Merchant Account: A special account with an acquiring bank that allows the merchant to accept credit cards over the Internet. The merchant typically pays a processing fee for each transaction processed, also known as the discount rate. A merchant applies for an Internet merchant account in a process similar to applying for a commercial loan. The fees charged by the acquiring bank will vary.

Merchant: Someone who owns a company that sells products or services.

Payment Gateway: A service that provides connectivity among merchants, customers, and financial networks to process authorizations and payments. The service is usually operated by a third-party provider such as VeriSign.

Processor: A large data center that processes credit card transactions and settles funds to merchants. The processor is connected to a merchant's site on behalf of an acquiring bank via a payment gateway.

Settlement: The process by which transactions with authorization codes are sent to the processor for payment to the merchant. Settlement is a sort of electronic bookkeeping procedure that causes all funds from captured transactions to be routed to the merchant's acquiring bank for deposit [2].

Controlling Access

One aspect of implementing a security policy is being able to control which users have access to particular systems and the data that they can access. There are a variety of security products for regulating the users allowed access to a system or providing the means to secure information by encryption. Some of these products will be discussed in detail later in the chapter and throughout the book [1].

Authenticated Access

When an user logs into a system, what measures can be taken to ensure that he is a valid user, as opposed to someone who has stolen a password? Within a company, card keys and security personnel can ensure that only employees are accessing its systems, but for remote users, there is a much higher perceived security risk. Many companies provide each of their remote users with a digital token card (also called hard tokens) to increase their assurance of the identity of each remote user [1].

Earlier in this chapter, mention was made of trusted third parties, called certificate authorities. Verisign is a commercial certification authority that issues digital certificates providing assurance of the identify of an individual. Typically a Verisign digital certificate contains the owner's public key, name, expiration date of public key, name of issuer (Verisign), serial number of the certificate, and Verisign's digital signature. Additional information may also be included, depending on the type of certificate. Verisign has facilities in California and Japan that issue digital certificates, provide digital identification for specific individuals, and maintain lists of revoked digital certificates [1].

Verisign provides two types of digital certificates: personal certificates to provide assurance of the identity of an individual and secure server certificates to protect communications with a given server and allow verification of the identity of a server. Its Class 1 personal certificates provide a unique name and email address within its repository. A Class 2 personal certificate requires confirmation of name, mailing address, and other personal information by an Equifax consumer database, along with a physical mail-back process to ensure that the request was not generated by someone with access to an applicant's personal information [1].

In the future, it is expected that there will be many certificate authorities available, ranging from banks to firms. The process of obtaining a certificate will be similar to that shown in Figure 3.3 [1].

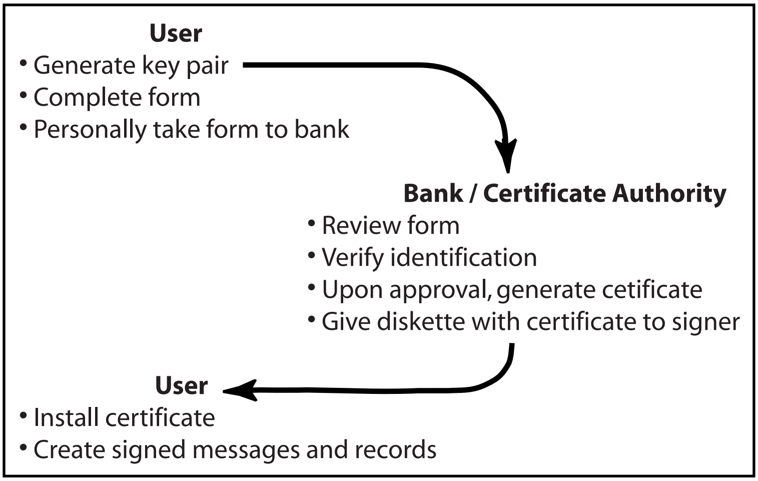

User
• Generate key pair
• Complete form
• Personally take form to bank
Bank / Certificate Authority
• Review form
• Verify identification
• Upon approval, generate cetificate
• Give diskette with certificate to signer
User
• Install certificate
• Create signed messages and records

FIGURE 3.3 Certification issuing process.

Privacy and Encryption

Another means of controlling access to information is to encrypt it. With a sufficiently long encryption key, the cost and time required to break the key will greatly exceed the value of the data. Encryption should only be used in a carefully thought out manner, as part of a security policy, not as a substitute [1].

For example, Pretty Good Privacy (PGP) is a program for protecting the privacy of email and computer files. It runs on virtually every platform. PGP provides the means for encrypting files and email, creating public and private keys, maintaining a database of public keys, adding digital signatures to documents, and to certifying keys and obtaining keys from key servers. In other words, PGP offers the advantage of running on a wide variety of systems and providing individuals with the ability to keep certain data confidential [1].

Secure Virtual Private Networks

Many corporate networks used for electronic data interchange (EDI) and funds transfer have been implemented using either private networks or costly services from specialized telecommunications network providers. Significant reduction in internal corporate networking costs can be achieved by using secure, encrypted, Internet protocol (IP)-level network communications over less expensive public networks, called secure virtual private networks (SVPN). Implementing such SVPNs requires authentication of the sources of all data, privacy from competitors and intruders, and assurance of the integrity of all data to minimize the possibility of fraud [1].

Security Futures: Smart Cards

Logically, a smart card is equivalent to an electronic safe deposit box. Implemented as a credit-card-sized piece of plastic, a smart card contains a semiconductor chip with logic and nonvolatile memory. The software within the card detects attempts at intrusion and tampering and monitors abnormal usage. Billions of smart cards have been made since their introduction in 1977. While smart cards are popular in Asia and Europe, they are just beginning to become popular here in the United States. Some of the many applications of smart cards include:

Stored value card: Minimizes the need to carry cash; can be used to purchase items from merchants, vending machines and pay phones.

Health care: Portable, customized health care file with medical emergency data and HMO and insurance information.

Access control in offices and hotels: Allows storage of time entered, exited, access conditions, and identity.

Contactless tickets for ski resorts and airlines: Increases speed, convenience, and security and facilitates baggage checking [1].

Smart cards can be read using conventional contact readers or interrogated remotely by microwave or infrared signals. They offer superior security and lower life cycle costs than alternatives such as coins, paper money, and magnetic stripe cards [1].

Security in smart cards is typically ensured by a combination of digital signature and public key technology. There are many different algorithms in use for smart cards, but all act to verify the authenticity of cards and to prevent misuse or fraud. Smart cards incorporate write-once memory that cannot be modified once it has been programmed, allowing each card to contain a unique identification number. Limits are typically placed on the number of erroneous attempts, preventing brute-force attempts [1].

Regarding computer forensics systems, this section has briefly touched on a wide variety of Internet security system topics involved with managing risk. Now let's move on to the next computer forensics system: intrusion detection systems.

INTRUSION DETECTION SYSTEMS

Intrusion detection systems help computer systems prepare for and deal with attacks. They collect information from a variety of vantage points within computer systems and networks and analyze this information for symptoms of security problems. Vulnerability assessment systems check systems and networks for system problems and configuration errors that represent security vulnerabilities. Both intrusion detection and vulnerability assessment technologies allow organizations to protect themselves from losses associated with network security problems. This section explains how intrusion detection and vulnerability assessment fits into the overall framework of security products and techniques used in computer forensics.

Protecting critical information systems and networks is a complex operation, with many tradeoffs and considerations. The effectiveness of any security solution strategy depends on selecting the right products with the right combination of features for the system environment one wishes to protect. This section also provides the information one needs to be a savvy consumer in the areas of intrusion detection and vulnerability assessment.

Intrusion Detection Defined

Intrusion detection systems help computer systems prepare for and deal with attacks. They accomplish this goal by collecting information from a variety of system and network sources and then analyzing the information for symptoms of security problems.

In some cases, intrusion detection systems allow the user to specify real-time responses to the violations. Intrusion detection systems perform a variety of functions:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis of abnormal activity patterns
- Operating system audit trail management, with recognition of user activity reflecting policy violations [3]

Some systems provide additional features, including

- Automatic installation of vendor-provided software patches
- Installation and operation of decoy servers to record information about intruders [3]

The combination of these features allows system managers to more easily handle the monitoring, audit, and assessment of their systems and networks. This ongoing assessment and audit activity is a necessary part of sound security management practice [3].

Vulnerability Assessment and Intrusion Detection

Vulnerability assessment products (also known as *scanners*) perform rigorous examinations of systems in order to determine weaknesses that might allow security violations. These products use two strategies for performing these examinations. First, *passive,* host-based mechanisms inspect system configuration files for unwise settings, system password files for weak passwords, and other system objects for security policy violations. These checks are followed, in most cases, by *active*, network-based assessment, which reenacts common intrusion scripts, recording system responses to the scripts [3].

The results of vulnerability assessment tools represent a snapshot of system security at a point in time. Although these systems *cannot* reliably detect an attack in progress, they *can* determine that an attack is possible, and furthermore, they *can sometimes* determine that an attack has occurred. Because they offer benefits that are similar to those provided by intrusion detection systems, they are included in the sphere of intrusion detection technologies and products [3].

Products Can Be Successfully Deployed in Operational Environments

The objective of intrusion detection and vulnerability assessment is to make complex, tedious, and sometimes virtually impossible system security management functions possible for those who are not security experts. Products are therefore designed with user-friendly interfaces that assist system administrators in their installation, configuration, and use. Most products include information about the problems they discover, including how to correct these problems, and provide valuable guidance for those who need to improve their security skills. Many vendors provide consulting and integration services to assist customers in successfully using their products to achieve their security goals [3].

Network Security Management

Network security management is a process in which one establishes and maintains policies, procedures, and practices required for protecting networked information system assets. Intrusion detection and vulnerability assessment products provide capabilities needed as part of sound network security management practice [3].

Why Firewalls Aren't Enough

A common question is how intrusion detection complements firewalls. One way of characterizing the difference is provided by classifying security violations by *source*—whether they come from outside the organization's network or from within. Firewalls act as a barrier between corporate (internal) networks and the outside world (Internet) and filter incoming traffic according to a security policy. This is a valuable function and would be sufficient protection were it not for these facts:

- Not all access to the Internet occurs through the firewall.
- Not all threat originates outside the firewall.
- Firewalls are subject to attack themselves [3].

Not All Access to the Internet Occurs Through the Firewall

Users, for a variety of reasons ranging from naiveté to impatience, sometimes set up unauthorized modem connections between their systems connected to the internal network and outside Internet access providers or other avenues to the Internet. The firewall cannot mitigate risk associated with connections it never sees [3].

Not All Threats Originate Outside the Firewall

A vast majority of loss from security incidents is traced to insiders. Again, the firewall only sees traffic at the boundaries between the internal network and the Internet. If the traffic reflecting security breaches never flows past the firewall, it cannot see the problems [3].

As more organizations utilize strong encryption to secure files and public network connections, the focus of adversaries will shift to those places in the network in which the information of interest is not as likely to be protected: the internal network. Intrusion detection systems are the only part of the infrastructure that is privy to the traffic on the internal network. Therefore, they will become even more important as security infrastructures evolve [3].

Firewalls Are Subject to Attack Themselves

Attacks and strategies for circumventing firewalls have been widely publicized since the first firewalls were fielded. A common attack strategy is to utilize *tunneling* to bypass firewall protections. Tunneling is the practice of encapsulating a message in one protocol (that might be blocked by firewall filters) inside a second message [3].

Trust and Intrusion Detection

Another area of discussion when considering the value of intrusion detection systems is the need to monitor the rest of the security infrastructure. Firewalls, identification and authentication products, access control products, virtual private networks, encryption products, and virus scanners all perform functions essential to system security. Given their vital roles, however, they are also prime targets of attack by adversaries. On a less sinister note, they are also managed by mere mortals and therefore subject to human error. Be it due to misconfiguration, outright failure, or attack, the failure of any of these components of the security infrastructure jeopardizes the security of the systems they protect [3].

By monitoring the event logs generated by these systems, as well as monitoring the system activities for signs of attack, intrusion detection systems provide an added measure of integrity to the rest of the security infrastructure. Vulnerability assessment products also allow system management to test new configurations of the security infrastructure for flaws and omissions that might lead to problems [3].

System Security Management: A Process View

Securing systems is not a point fix. It is an ongoing process targeting a dynamic environment in which new threats arise daily [3].

Prevention covers those proactive measures taken by organizations to mitigate risks to their system security. Much of the classic, government-sponsored work in computer security addresses this area by focusing on the design and implementation of more secure operating systems and applications software. Prevention also includes security policy formation, encryption, strong identification and authentication, and firewalls [3].

Functions in the detection phase are primarily provided by intrusion detection systems, although virus scanners also fall into this category. Thus, detection involves monitoring the targeted system(s), analyzing the information gathered for problems, and then, based on the system settings, responding to the problems, reporting the problems, or both [3].

The results of the detection process drive the other two stages of managing security: (a) investigating problems that are discovered and documenting the cause of the problem and (b) either correcting the problem or devising a means of dealing with it should it occur again. A common vision for future intrusion detection systems is that of performing these last two stages automatically, or else performing the functions internal to detection so well that the need for the last two stages is virtually eliminated [3].

The combination of the investigation and diagnosis/resolution phases is often called *incident response* or *incident handling*. Organizations should specify policies, procedures, and practices to address this area as it does the rest of security [3].

What Intrusion Detection Systems and Related Technologies Can and Cannot Do

Every new market suffers from exaggeration and misconception. Some of the claims made in marketing materials are reasonable and others are misleading. Here is a primer on how to read intrusion detection marketing literature [3].

Realistic Benefits

First of all, intrusion detection systems (IDSs) can lend a greater degree of integrity to the rest of your security infrastructure. The reason for this is because they monitor the operation of firewalls, encrypting routers, key management servers and files critical to other security mechanisms, thus providing additional layers of protection to a secured system. Therefore, the strategy of a system attacker will often include attacking or otherwise nullifying security devices protecting the intended target. Intrusion detection systems can recognize these first hallmarks of attack and potentially respond to them, mitigating damage. In addition, when these devices fail, due to configuration, attack, or user error, intrusion detection systems can recognize the problem and notify the right people [3].

Second, intrusion detection systems can also make sense of often obtuse system information sources, telling you what's really happening on your systems. Operating system audit trails and other system logs are a treasure trove of information about what's going on internal to your systems. They are also often incomprehensible, even to expert system administrators and security officers. Intrusion detection systems allow administrators and managers to tune, organize, and comprehend what these information sources tell them, often revealing problems before loss occurs [3].

Third, intrusion detection systems can also trace user activity from the point of entry to the point of exit or impact. Intrusion detection systems offer improvements over perimeter protections such as firewalls. Expert attackers can often penetrate firewalls; therefore, the ability to correlate activity corresponding to a particular user is critical to improving security [3].

Fourth, intrusion detection systems can recognize and report alterations to data files. Putting trojan horses in critical system files is a standard attack technique. Similarly, the alteration of critical information files to mask illegal activity, damage reputations, or commit fraud is common. File integrity assessment tools utilize strong cryptographic checksums to render these files tamper-evident and, in the case of a problem, quickly ascertain the extent of damage [3].

Fifth, intrusion detection systems can also spot errors of your system configuration that have security implications, sometimes correcting them if the user wishes. Vulnerability assessment products allow consistent auditing and diagnosis of system configuration settings that might cause security problems. These products offer extensive vendor support and turnkey design so that even novice security personnel can look for hundreds of problems by pushing a button. Some of these product offerings even offer automated fixes for the problems uncovered [3].

Sixth, intrusion detection systems can recognize when your system appears to be subject to a particular attack. Vulnerability assessment products also allow the user of a system to quickly determine what attacks should be of concern to that system. Again, strong vendor support allows novice security personnel to reenact scores of hacker attacks against their system, automatically recording the results of these attack attempts. These products also provide a valuable sanity check for those installing and setting up new security infrastructures. It is far better for a system manager to determine that his or her firewall is incorrectly configured immediately than to discover this after an attacker has successfully penetrated it [3].

Seventh, intrusion detection systems can relieve your system management staff of the task of monitoring the Internet, searching for the late hacker attacks. Many intrusion detection and assessment tools come with extensive attack signature databases against which they match information from your system. The firms developing these products have expert staffs that monitor the Internet and other sources for reports and other information about new hacker attack tools and techniques. They then use this information to develop new signatures that are provided to customers for download from Web sites, downloaded to customers via encrypted email messages, or both [3].

Eighth, intrusion detection systems can make the security management of your systems by nonexpert staff possible. Some intrusion detection and assessment tools offer those with no security expertise the ability to manage security-relevant features of your systems from a user-friendly interface. These are window-based, point-and-click screens that step users through setup and configuration in a logical, readily understood fashion [3].

Finally, intrusion detection systems can provide guidelines that assist you in the vital step of establishing a security policy for your computing assets. Many intrusion detection and assessment products are part of comprehensive security suites that include security policy building tools. These provide easy-to-understand guidance in building your security policy, prompting you for information and answers that allow you to articulate goals and guidelines for the use of your computer systems [3].

Unrealistic Expectations

First, intrusion detection systems are not silver bullets. Security is a complex area with myriad possibilities and difficulties. In networks, it is also a “weakest link” phenomenon (it only takes one vulnerability on one machine to allow an adversary to gain entry and potentially wreak havoc on the entire network). The time it takes for this to occur is minuscule. There are no magic solutions to network security problems, and intrusion detection products are no exception to this rule. However, as part of a comprehensive security management they can play a vital role in protecting your systems [3].

Second, intrusion detection systems cannot compensate for weak identification and authentication mechanisms. Although leading-edge research in intrusion detection asserts that sophisticated statistical analysis of user behavior can assist in identification of a particular person by observing their system activity, this fact is far from demonstrated. Therefore, you must still rely on other means of identification and authentication of users. This is best accomplished by strong authentication mechanisms (including token-based or biometric schemes and one-time passwords). A security infrastructure that includes strong identification and authentication *and* intrusion detection is stronger than one containing only one or the other [3].

Third, intrusion detection systems cannot conduct investigations of attacks without human intervention. In very secure environments, incidents happen. In order to minimize the occurrence of incidents (and the possibility of resulting damage) one must perform *incident handling*. One must investigate the attacks, determine, where possible, the responsible party, and then diagnose and correct the vulnerability that allowed the problem to occur, reporting the attack and particulars to authorities where required. In some cases, especially those involving a dedicated attacker, finding the attacker and pursuing criminal charges against the attacker is the only way to make the attacks cease. However, the intrusion-detection system is not capable of identifying the person at the other end of the connection without human intervention. The best that it can do is identify the IP address of the system that served as the attacker’s point of entry—the rest is up to a human incident handler [3].

Fourth, intrusion detection systems cannot intuit the contents of your organizational security policy. Intrusion-detection expert systems increase in value when they are allowed to function as both hacker/burglar alarms and policy-compliance engines. These functions cannot only spot the high-school hacker executing the “teardrop” attack against your file server, but also spot the programmer accessing the payroll system after hours. However, this policy compliance checking can exist only if there is a security policy to serve as a template for constructing detection signatures [3].

Fifth, intrusion detection systems cannot compensate for weaknesses in transmission control protocol (TCP)/IP, and many other network protocols do not perform strong authentication of host source and destination addresses. This means that the source address that is reflected in the packets carrying an attack does not necessarily correspond to the *real* source of the attack. It is difficult to identify who is attacking one's system; it is very difficult to prove the identity of an attacker in a court of law—for example, in civil or criminal legal processes [3].

Sixth, intrusion detection systems cannot compensate for problems in the quality or integrity of information the system provides. In other words, "garbage in garbage out" still applies. System information sources are mined from a variety of points within the system. Despite the best efforts on the part of system vendors, many of these sources are software-based; as such, the data are subject to alteration by attackers. Many hacker tools (for example "cloak" and "zap") explicitly target system logs, selectively erasing records corresponding to the time of the attack and covering the intruders' tracks. This argues for the value of integrated, sometimes redundant, information sources; each additional source increases the possibility of obtaining information not corrupted by an attacker [3].

Seventh, intrusion detection systems cannot analyze all of the traffic on a busy network. Network-based intrusion detection is capable of monitoring traffic on a network, but only to a point. Given the vantage point of network-based intrusion detection sources that rely on network adapters set to promiscuous mode, not all packets are visible to the systems. Also, as traffic levels rise, the associated processing load required to keep up becomes prohibitive and the analysis engine either falls behind or fails. In fact, vendors themselves characterized the maximum bandwidth at which they had demonstrated their products to operate without loss with 100% analysis coverage at 65 MB/sec [3].

Eighth, intrusion detection systems cannot always deal with problems involving packet-level attacks. There are weaknesses in packet-capture-based network intrusion detection systems. The heart of the vulnerabilities involves the difference between the intrusion detection systems' interpretation of the outcome of a network transaction (based on its reconstruction of the network session) and the destination node for that network session's actual handling of the transaction. Therefore, a knowledgeable adversary can send series of fragmented and otherwise doctored packets that elude detection but launch attacks on the destination node. Worse yet, an adversary can use this sort of packet manipulation to accomplish a denial of service attack on the intrusion detection systems itself by overflowing memory allocated for incoming packet queues [3].

Finally, intrusion detection systems cannot deal with modern network hardware and features. Dealing with fragmented packets can also be problematic. This problem has serious ramifications when one considers modern high-speed asynchronous transfer mode (ATM) networks that use packet fragmentation as a means of optimizing bandwidth. Other problems associated with advances in network technologies include the effect of switched networks on packet-capture-based network intrusion detection systems. As the effect of switched networks is to establish a network segment for each host, the range of coverage for a network intrusion system is reduced to a single host. This problem can be mitigated in those switches offering monitoring ports or spanning capability; however, these features are not universal in current equipment [3].

The capabilities for intrusion detection are growing as new technologies enter the marketplace and existing organizations expand their product offerings to allow additional sensor inputs, improved analysis techniques, and more extensive signature databases. Thanks to government and military interest in information warfare (discussed in Chapters 13 to 19), of which intrusion detection is a vital defensive component, funding of research efforts has skyrocketed, with no end in sight. This increased activity will result in enhanced understanding of the intrusion detection process and new features in future products. Intrusion detection products have now been embedded as standard components of major governmental and financial networks [3].

As intrusion detection remains an active research area, look for future technologies to implement new techniques for managing data and detecting scenarios of interest. Also look for products that function at application level and that interoperate with network management platforms. Finally, look for product features that are integrated into a bevy of special purpose devices, ranging from bandwidth management products to "black box" plug-ins for targeted environments [3].

FIREWALL SECURITY SYSTEMS

Today, when an organization connects its private network to the Internet, security has to be one of primary concerns. In the past, before the widespread interest in the Internet, most network administrators were concerned about attacks on their networks from within, perhaps from disgruntled workers. For most organizations now connecting to the Internet and big business and big money moving toward electronic commerce at warp speed, the motive for mischief from outside is growing rapidly and creating a major security risk to enterprise networks.

Reacting to this threat, an increasing number of network administrators are installing the latest firewall technology as a *first line of defense* in the form of a barrier against outside attacks. These firewall gateways provide a choke point at which security and auditing can be imposed. They allow access to resources on the Internet from within the organization while providing controlled access from the Internet to hosts inside the virtual private network (VPN).

The threat of attack on your network increases proportionally with the continued exponential growth of the Internet. If it is necessary for you to connect your network to the Internet, an appropriate security protocol should be decided on and implemented. This book illustrates many reasons why this is necessary, as well as many techniques to consider for your firewall solution. The bottom line is, do not connect your network to the Internet without some sort of protection. Also, do not put sensitive information in a place where it can be accessed over the Internet. The firewall you decide to use will prevent most of the attacks on your network; however, firewalls will not protect against dial-in modem attacks, virus attacks, or attacks from within your company.

Nevertheless, a number of the security problems with the Internet can be remedied or made less serious through the use of existing and well-known techniques and controls for host security. A firewall can significantly improve the level of site security while at the same time permitting access to vital Internet services. This section provides an overview of firewall technology, including how they protect against vulnerabilities, what firewalls don't protect against, and the components that make up a firewall.

Firewall Defined

A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one that blocks traffic and one that permits traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy. If you don't have a good idea what kind of access you want to permit or deny, or you simply permit someone or some product to configure a firewall based on what they or it think it should do, then they are making policy for your organization as a whole.

In other words, a firewall is a network security product that acts as a barrier between two or more network segments. The firewall is a system (which consists of one or more components) that provides an access control mechanism between your network and the network(s) on the other side(s) of the firewall. A firewall can also provide audit and alarm mechanisms that will allow you to keep a record of all access attempts to and from your network, as well as a real-time notification of things that you determine to be important.

Perhaps it is best to describe first what a firewall is not: a firewall is not simply a router, host system, or collection of systems that provides security to a network. Rather, a firewall is an approach to security; it helps implement a larger security policy that defines the services and access to be permitted, and it is an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall system is to control access to or from a protected network (a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

A firewall system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnet. A firewall system is usually located at a higher-level gateway, such as a site's connection to the Internet. However, firewall systems can be located at lower-level gateways to provide protection for some smaller collection of hosts or subnets.

Why do we need firewalls? What can a firewall do for you? Why would you want a firewall? What can a firewall not do for you? All of these burning questions are answered next for *those inquiring security minds that want to know.*

The Reason for Firewalls

The general reasoning behind firewall usage is that without a firewall, a subnet's systems are exposed to inherently insecure services such as Network File System (NFS) or Network Information Service (NIS) and to probes and attacks from hosts elsewhere on the network.

In a firewall-less environment, network security relies totally on host security, and all hosts must, in a sense, cooperate to achieve a uniformly high level of security. The larger the subnet, the less manageable it is to maintain all hosts at the same level of security. As mistakes and lapses in security become more common, break-ins occur not as the result of complex attacks, but because of simple errors in configuration and inadequate passwords.

The Need For Firewalls

As technology has advanced to greatly expand the information technology systems capabilities of corporations, the threats to these systems have become numerous and complex. In today's world, corporations face a variety of information system attacks against their local area networks (LANs) and wide area networks (WANs). Many of these attacks are directed through the Internet. These attacks come from three basic groups:

- Persons who see attacking a corporation's information system as a technological challenge
- Persons with no identified political or social agenda who see attacking a corporation's information system as an opportunity for high-tech vandalism
- Persons associated with a corporate competitor or political adversary who see the corporation's information system as a legitimate strategic target

To combat this growing and complex threat to a corporation's LAN and Internet site, a series of protective countermeasures needs to be developed, continually updated, and improved. Security services that are important to protecting a corporation's strategic information include:

Data Integrity: Absolute verification that data has not been modified

Confidentiality: Privacy with encryption, scrambled text

Authentication: Verification of originator on contract

Non-Repudiation: Undeniable proof-of-participation

Availability: Assurance of service demand

It's really the endpoints, like the servers, on your network you need to secure right? After all, that's where the sensitive data lives. You've got password protection on your servers and you've implemented other security measures on your servers as well. You may even have an administrator for your servers who is security-savvy; however, are you willing to bet your company's private information in this way?

The building and implementation of firewalls is an effective security countermeasure used to implement these security services. An external firewall is used to counter threats from the Internet. An internal firewall is primarily used to defend a corporation's LAN or WAN. The internal firewall is used to separate and protect corporate databases (for example, financial databases can be separated from personnel databases). In addition, internal firewalls can be used to separate different levels of information being sent over a corporate LAN or WAN (for example, corporate proprietary information dealing with research projects, financial data, or personnel records).

Firewalls, however, are just one element in an array of possible information technology (IT) systems countermeasures. The most effective security countermeasure is a good corporate security strategy. The effectiveness of this strategy will have a direct bearing on the success of any firewall that a corporation builds or purchases. For example, the two critical elements that form the basis of an effective corporate security strategy are: *least privilege* and *defense in depth*.

Least Privilege

The principle of least privilege means that an object is given only the privileges it needs to perform its assigned tasks. Least privilege is an important principle in countering attacks and limiting damage.

Defense in Depth

Don't depend on one security solution. Good security is usually found in layers. These layers should consist of a variety of security products and services. The solutions could be network security products (firewalls that could be both internal and external) and information systems security (INFOSEC) training (employee education through classes and threat and vulnerability briefings).

Do you want to let them even begin to work against your server's security? Isn't it possible that your administrator might go home at night and miss the attack? Can't human errors in password security be made now and then? Firewalls are de-

signed to allow you a very important second layer of protection. Detection of security problems can be made at this layer before any security breach can begin on any of your data-sensitive servers.

A firewall approach provides numerous advantages to sites by helping to increase overall host security. The following provides an overview of the primary benefits of using a firewall.

Benefits of Firewalls

A firewall provides a leveraged choke point for network security. It allows the corporation to focus on a critically vulnerable point: where the corporation's information system connects to the Internet. The firewall can control and prevent attacks from insecure network services. A firewall can effectively monitor all traffic passing through the system. In this manner, the firewall serves as *an auditor* for the system and can alert the corporation to anomalies in the system. The firewall can also log access and compile statistics that can be used to create a profile of the system.

Some firewalls, on the other hand, permit only email traffic through them, thereby protecting the network against any attacks other than attacks against the email service. Other firewalls provide less strict protections and block services that are known to be problems.

Generally, firewalls are configured to protect against unauthenticated interactive logins from the *outside* world. This, more than anything, helps prevent vandals from logging into machines on your network. More elaborate firewalls block traffic from the outside to the inside but permit users on the inside to communicate freely with the outside..

Firewalls are also important since they can provide a single *choke point* where security and audit can be imposed. Unlike in a situation where a computer system is being attacked by someone dialing in with a modem, the firewall can act as an effective *phone tap* and tracing tool. Firewalls provide an important logging and auditing function. Often, they provide summaries to the administrator about what kinds and amount of traffic passed through it, how many attempts there were to break into it, etc. The following are the primary benefits of using a firewall:

- Protection from vulnerable services
- Controlled access to site systems
- Concentrated security
- Enhanced privacy
- Logging and statistics on network use and misuse
- Policy enforcement

Protection from Vulnerable Services

A firewall can greatly improve network security and reduce risks to hosts on the subnet by filtering inherently insecure services. As a result, the subnet network environment is exposed to fewer risks, since only selected protocols will be able to pass through the firewall.

For example, a firewall could prohibit certain vulnerable services such as NFS from entering or leaving a protected subnet. This provides the benefit of preventing the services from being exploited by outside attackers, but at the same time permits the use of these services with greatly reduced risk to exploitation. Services such as NIS or NFS that are particularly useful on a LAN basis can thus be enjoyed and used to reduce the host management burden.

Firewalls can also provide protection from routing-based attacks, such as source routing and attempts to redirect routing paths to compromised sites via Internet control message protocol (ICMP) redirects. A firewall could reject all source-routed packets and ICMP redirects and then inform administrators of the incidents.

Controlled Access to Site Systems

A firewall also provides the ability to control access to site systems. For example, some hosts can be made reachable from outside networks, whereas others can be effectively sealed off from unwanted access. A site could prevent outside access to its hosts except for special cases such as email servers or information servers.

This brings to the fore an access policy that firewalls are particularly adept at enforcing: do not provide access to hosts or services that do not require access. Put differently, why provide access to hosts and services that could be exploited by attackers when the access is not used or required? If, for example, a user requires little or no network access to his or her desktop workstation, then a firewall can enforce this policy.

NOTE

ICMP is an extension to the IP defined by RFC 792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Concentrated Security

A firewall can be less expensive for an organization, in that all or most modified software and additional security software could be located on the firewall systems as opposed to being distributed on many hosts. In particular, one-time password systems and other add-on authentication software could be located at the firewall as opposed to on each system that needed to be accessed from the Internet.

Other solutions to network security such as Kerberos involve modifications at each host system. While Kerberos and other techniques should be considered for their advantages and may be more appropriate than firewalls in certain situations, firewalls tend to be simpler to implement in that only the firewall need run specialized software.

NOTE

Kerberos is an authentication system developed at the Massachusetts Institute of Technology (MIT). Kerberos is designed to enable two parties to exchange private information across an otherwise open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message.

Enhanced Privacy

Privacy is of great concern to certain sites, since what would normally be considered innocuous information might actually contain clues that would be useful to an attacker. Using a firewall, some sites wish to block services such as finger and Domain Name Service (DNS). Finger displays information about users such as their last login time, whether they've read mail, and other items, but, finger could leak information to attackers about how often a system is used, whether the system has active users connected, and whether the system could be attacked without drawing attention.

Firewalls can also be used to block DNS information about site systems; thus, the names and IP addresses of site systems would not be available to Internet hosts. Some sites feel that by blocking this information, they are hiding information that would otherwise be useful to attackers.

Logging and Statistics on Network Use and Misuse

If all access to and from the Internet passes through a firewall, the firewall can log accesses and provide valuable statistics about network usage. A firewall with appropriate alarms that sound when suspicious activity occurs can also provide details on whether the firewall and network are being probed or attacked.

It is important to collect network usage statistics and evidence of probing for a number of reasons. Of primary importance is knowing whether the firewall is withstanding probes and attacks and determining whether the controls on the firewall are adequate. Network usage statistics are also important as input into network requirements studies and risk analysis activities.

Policy Enforcement

Lastly, but perhaps most importantly, a firewall provides the means for implementing and enforcing a network access policy. In effect, a firewall provides access control to users and services. Thus, a network access policy can be enforced by a firewall, whereas without a firewall, such a policy depends entirely on the cooperation of users. A site may be able to depend on its own users for their cooperation, but it cannot and should not depend on Internet users in general.

There are also a number of disadvantages to the firewall approach, and there are a number of things that firewalls cannot protect against. A firewall is not by any means a panacea for Internet security problems.

Limitations of Firewalls

Firewalls can't protect against attacks that don't go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape can just as effectively be used to export data. Many organizations that are terrified (at a management level) of Internet connections have no coherent policy about how dial-in access via modems should be protected. It's silly to build an 8-foot-thick steel door when you live in a wooden house. There are a lot of organizations out there buying expensive firewalls and neglecting the numerous other back-doors into their networks. For a firewall to work, it must be a part of a consistent overall organizational security architecture. Firewall policies must be realistic and reflect the level of security in the entire network. For example, a site with top secret or classified data doesn't need a firewall at all: they shouldn't be hooking up to the Internet in the first place; or the systems with the really secret data should be isolated from the rest of the corporate network.

Another thing a firewall can't protect you against is traitors or idiots inside your network. While an industrial spy might export information through your firewall, he or she is just as likely to export it through a telephone, fax machine, or floppy disk. Floppy disks are a far more likely means for information to leak from your organization than a firewall. Firewalls also cannot protect you against stupidity. Users who reveal sensitive information over the telephone are good targets for social engineering. An attacker may be able to break into your network by completely bypassing your firewall if he or she can find a *helpful* employee inside who can be fooled into giving access to a modem pool.

A firewall opens communications channels between two networks and has no control over what users choose to transmit using these channels. It has no concept of the value or sensitivity of the data it is transferring between networks and therefore cannot protect information on that basis. A firewall cannot control what a user chooses to do with the data once he has received it. If a user chooses to modify or propagate that information, the firewall has no effect.

A firewall can protect the integrity of information from the time that it receives the information until it releases it on the other network. It cannot, however, test or ensure information integrity before it receives it or after it releases it. It also cannot prevent trusted users from disclosing (either accidentally or deliberately) information if they chose to do so.

A firewall cannot provide access control on any of your inside systems from someone already inside the firewall. If someone has already bypassed your firewall or is physically located on your inside network, then access attempts to your inside systems no longer need to go through the firewall, and the firewall will provide no protection. Finally, a firewall cannot completely protect your systems from data-driven attacks such as viruses.

Viruses

Firewalls can't protect very well against things like viruses. There are too many ways of encoding binary files for transfer over networks and too many different architectures and viruses to try to search for them all. In other words, a firewall cannot replace security-consciousness on the part of your users. In general, a firewall cannot protect against a data-driven attack—attacks in which something is mailed or copied to an internal host, where it is then executed. This form of attack has occurred in the past against various versions of Sendmail and GhostScript, a freely available PostScript viewer.

NOTE

Data-driven attacks are those that are transferred as data to the target system by user applications such as FTP, WWW, and email. This type of attack includes malicious programs, viruses, and Web applets. A firewall cannot completely eliminate the threat of this type of attack. Some restrictions may be put in place to limit the types of data that are received; however, they cannot be completely eliminated by a firewall, and user awareness and host-based virus scanning is important.

Organizations that are deeply concerned about viruses should implement organization-wide virus control measures. Rather than trying to screen viruses out at the firewall, make sure that every vulnerable desktop has virus scanning software that runs when the machine is rebooted. Blanketing your network with virus scanning software will protect against viruses that come in via floppy disks, modems, and the Internet. Trying to block viruses at the firewall will only protect against viruses from the Internet—and the vast majority of viruses are caught via floppy disks.

As previously discussed, a firewall is a system or group of systems that enforces an access control policy between two networks. There are many ways to implement firewalls on today's corporate networks. Usually they can be thought of as two mechanisms: one that permits traffic and one that blocks traffic. Whether a company wishes to place more emphasis on permitting or blocking traffic is up to the individuals who set the security policies for that company. A company should not leave this to the discretion of the service or product that will supply their security because only the company knows what kind of protection it needs. If a company is unsure about what kind of protection is necessary, there are numerous vendors who will help in setting up a secure network.

Firewalls are designed to protect your network from attacks originating from another network. An effective firewall will only allow authorized access to the protected network and will deny access to those who don't have authorized access. Some firewalls permit only email traffic through them, thereby protecting the network against any attacks other than attacks against the email service. Other firewalls provide less strict protections and block services that are known to be problems. A more effective firewall will allow users on the protected network to communicate freely with the outside world; this is the reason a company connects its LAN to the Internet. If a company wants to monitor the types and amounts of traffic that are directed at their network, a firewall can effectively supply this information to the system administrator.

A firewall will not block attempts to break into a network that come from external modems or from internal attacks. In other words, a firewall will not protect against any other attacks except for those originating from external networks. If a company has top secret information that it wants to keep secret, it should not connect any machines containing this information to the Internet. This is probably the most effective firewall to implement. Most companies would like to have some kind of Internet access available to their employees. If this is the case, then a firewall implemented at the application level will be able to supply the amount of security necessary to meet the company's needs.

Finally, leaks of information are far more likely to walk out the front door of the office on a floppy disk than over the Internet through your firewall.

STORAGE AREA NETWORK SECURITY SYSTEMS

In the aftermath of the devastation that occurred when the World Trade Center collapsed, disaster recovery services used storage area networks (SANs) to restore thousands of terabytes of business data and get hundreds of companies running. As distasteful as the idea might be, with disaster comes opportunity, and the disasters of September 11, 2001, provided a good opportunity for storage networks to show their value by providing critically important business continuity. Rarely has technology demonstrated its value in a more demanding environment.

Today, organizations continue to expose their IT systems to a wide range of potential security threats as they continue to broaden their reach to business partners and customers around the globe. Furthermore, data theft, eavesdropping, fraud, and hacker attempts increasingly threaten secure electronic information exchange within the enterprise and across public networks (such as the Internet).

Because IT systems are only as secure as the weakest link in the network, organizations need to consider outsourcing their data storage security needs to one vendor, which will help them develop a comprehensive security plan and architecture that helps ensure safe, reliable data processing throughout a SAN. In other words, an organization needs an integrated solution that addresses a wide variety of potential security threats—thus enabling a robust, mission-critical SAN infrastructure. Nevertheless, demand for high-availability SANs and disaster recovery technology is soaring as companies realize their IT dependency.

Storage Area Network Overview

SANs are a relatively new methodology for attaching storage, whereby a separate network (separate from the traditional LAN) connects all storage and servers. This network would be a high-performance implementation, such as a fiber channel, that encapsulates protocols such as a small computer system interface (SCSI). These are more efficient at transferring data blocks from storage and have hardware implementations offering buffering and delivery guarantees. This is not available using TCP/IP.

The SAN development areas have not yet been realized, but there is great potential with regard to centralized storage SAN management and storage abstraction. Storage abstraction refers to an indirect representation of storage that has also been called virtualization. Together with these potential enhancements, SANs should be able to generate greater functionality than has been possible previously. Thus, most system vendors have ambitious strategies to change the way enterprise operations store and manage data with new capabilities based on SANs.

As an alternative to the centralized arrays and tape libraries commonly deployed in data center storage consolidation strategies today, SANs are a new paradigm that allows the use of cost-effective modular arrays and tape libraries. Conversely, in order to amortize the cost of the storage over many servers, SANs are also being used to provide increased server connectivity to centralized arrays and tape libraries.

Due to the maturation of newer storage interconnect technologies like fibre channels, SANs are evolving. This solution holds perhaps the greatest promise for the storage-centric model of computing as shown in Figure 3.4.

SANs promise the ability to make any-to-any connections among multiple servers and storage devices. They can create a shared “pool” of storage that can be accessed by multiple servers through multiple paths, resulting in higher availability—especially during a network disaster recovery (NDR).

SANs also promise to simplify backup procedures. Tape subsystems could still be shared among numerous servers during backups—all transparent to the user. In other words, SANs allow distributed servers to access a large centralized storage subsystem for data-sharing applications during an NDR.

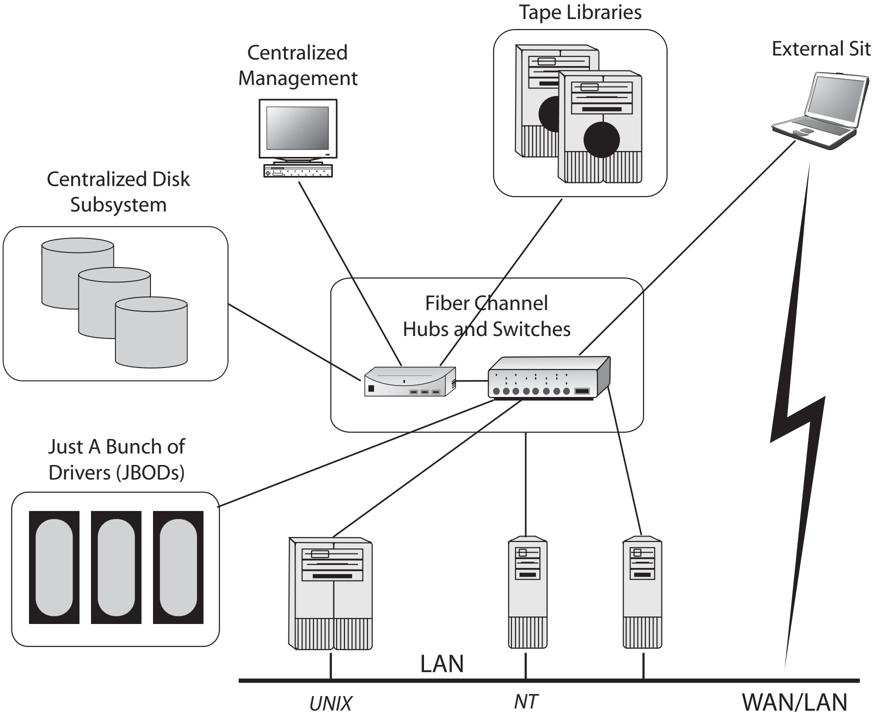

Tape Libraries
External Site
Centralized Management
Centralized Disk Subsystem
Fiber Channel Hubs and Switches
Just A Bunch of Drivers (JBODs)
LAN
UNIX
NT
WAN/LAN

FIGURE 3.4 Storage-centric model of computing

Devices could also be distributed throughout a campus yet managed from a central point though a single management tool. Since devices can be added or reconfigured transparently with location flexibility, scaling the SAN will be easy.

SAN Benefits

A SAN provides a perfect environment for clustering that can extend to dozens of servers and storage devices—all the while having redundant links in a fibre channel fabric. Servers will continue to function because their data is still available through the SAN, even if storage devices fail during an NDR.

Centralized Management

When a disk or controller fails in a direct-attached environment, redundant systems keep the redundant array of independent (or inexpensive) disks (RAID) array operating normally and generate an alarm. However, the redundant component may fail as well, bringing the system down if the failed component isn't replaced quickly. Also, the chances are good that because of human error or inefficient management practices, an alarm will eventually be missed and a storage subsystem will fail in an enterprise with a large number of RAID subsystems managed in a decentralized fashion.

From one management console, a centralized pool of storage can be managed more efficiently. Everyday administrative tasks can be centrally managed. This lowers the costs of storage management and significantly increases the consistency and span of control of system administrators, as well as increasing the availability of data during an NDR.

Scalability

A storage area network can lower acquisition and expansion costs, in addition to lowering management costs. Even as new servers, disk arrays, and tape subsystems are added, the SAN architecture supports access between all servers and all storage resources in the network. Without disrupting data access, customers can add storage resources and even servers online. For example, additional tape libraries can be added to the SAN and will be available to all systems and the backup application, even if increasing disk capacity makes backup times exceed the time window allotted.

Reliability

A SAN is a network that resides between the host bus adapter and the storage device. This position inherently creates a critical point at the physical level, but by implementing multiple paths and redundant infrastructure devices, the SAN reduces or eliminates single points of failure. Because monitoring of the network is much easier now, centralization facilitates more rigorous, consistent management practices and thus increases the overall reliability.

Performance

In application environments that depend on bulk data transfer (such as data warehousing and data-mining applications), maximum bandwidth is of particular interest. Current fibre channel connections can support 400 MB/sec and greater data-transfer rates for faster access to more storage resources than they do for server-attached or LAN-attached storage today. Backup and restore times can be shortened dramatically by the high channel speed and low latency obtained by using a SAN.

Making it possible to access more devices at one time is another way that a SAN can improve performance. For example, the backup task can be accomplished even more quickly if the SAN makes it possible to back up application data utilizing up to eight tape drives simultaneously.

SANs aren’t the only alternative storage solution during an NDR, but they are the best alternative available today. Let’s now look at NDR systems as part of computer forensics systems.

NETWORK DISASTER RECOVERY SYSTEMS

The high availability of mission-critical systems and communications is a major requirement for the viability of the modern organization. A network disaster could negate the capability of the organization to provide uninterrupted service to its internal and external customers.

How would your company respond in the event of a network disaster or emergency? Network disaster recovery (NDR) is the ability to respond to an interruption in network services by implementing a disaster recovery plan to restore an organization's critical business functions. NDR is not a new idea. In recent years, data has become a vitally important corporate asset essential to business continuity. A fundamental requirement of economic viability is the ability to recover crucial data quickly after a disaster.

While the great majority of companies have plans for NDR in place, those without an NDR plan indicate that they intend to create one. Is *intend to create one* good enough to make sure the critical parts of your business will be able to continue to function in the event of a catastrophe? You will have to take the time to determine, in partnership with your executive committee, exactly what it means for your firm to be *very prepared*. Staff training is clearly the greatest missing link in disaster recovery preparations. The next most important issue is backing up corporate data more frequently.

Many companies see their disaster recovery efforts as being focused primarily on their IT departments. IT people are in the lead in sponsoring and managing their disaster recovery plans, and relatively few companies involve line-of-business staff and partners in designing and testing such plans at all. Not surprisingly, the person most frequently cited as being responsible for the management of an NDR plan is the company's chief information officer (CIO) or another IT manager.

There's general agreement on what should be covered in an NDR plan. Network outages are the number-one issue for smaller companies and high on the list for larger companies. This puts a premium on reliable networking hardware and software. Natural disasters also ranked high. At the bottom of the list are attacks on company Web sites, employee-initiated outages, and service provider failures.

Larger companies (those with $20 million or more in annual revenues) are more likely than smaller companies to prepare for events such as hardware component failure versus natural disasters and accidental employee-initiated outages. The most frequent services include regular off-site data backups and virus detection and protection.

As for components that are or will be part of their NDR plan, larger businesses are more likely to perform or plan to perform a business impact analysis than smaller firms. However, most companies cite components such as a process for administering the NDR plan, setting out what individuals should do in the aftermath of a disaster, and recovery strategies.

A majority of companies indicate they review their NDR plans every quarter, but some companies haven't reviewed their plans at all. Testing, however, appears to be done less often. The data center is the most frequently tested plan component. A few businesses are showing increased interest in testing their NDR plans more often than they have in the past.

The impact of the loss of mission-critical systems naturally varies depending on a company's size. Companies with more than $30 million in annual revenues have indicated they have losses in excess of $300,000 per day.

Major hardware component failure and a network failure are the most common problems. That provides strong support for the usual reported focus on the kinds of problems companies are most intent on avoiding, but most of these can't have been major breaches. Most companies believe they don't have to worry about being offline for long. Most companies have their mission-critical systems back up within 24 hours.

SANs offer the most promising solutions for storage problems today, complementing the other solutions of direct storage, centralized storage, and network-attached storage.

Even before the events of 9/11, most companies were taking NDR planning seriously. The majority seemed to be following reasonably good planning practices, focusing on major potential sources of problems.

Large companies, certainly, have more incentive to plan and test more completely; as well as the resources to do so, but even smaller companies have given at least some thought to the problem. Thus, there's a potential disconnect in terms of perception. IT organizations must focus far more on involving partners, suppliers, and other members of the organization in any future plan.

PUBLIC KEY INFRASTRUCTURE SYSTEMS

To mitigate the security risks of conducting business in an open environment while at the same time maintaining the cost advantages of doing so, enterprises are turning their attention to an emerging segment of the security market known as public key infrastructure (PKI). The purpose of PKI is to provide an environment that addresses today's business, legal, network, and security demands for trust and confidentiality in data transmission and storage. PKI accomplishes these goals for an enterprise through policy and technology components. These components determine and identify the roles, responsibilities, constraints, range of use, and services available. This section briefly identifies the key concepts and issues surrounding the technologies and policies required to implement and support an enterprise PKI.

In other words, PKI is a system for supporting digital signatures and document encryption for an organization. It is fast becoming essential for effective, secure e-commerce and to fulfill general security and authentication requirements over nonsecure networks (like the Net). The banking services are the most popular usage of this technology, which is quickly spreading over all the applications that need security to be fully operational.

PKI Defined

A PKI enables users of an insecure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The PKI provides for digital certificates that can identify individuals or organizations and directory services that can store and, when necessary, revoke them. PKI is the underlying technology that provides security for the secure sockets layer (SSL) and hyper text transfer protocol secure sockets (HTTPS) protocols, which are used extensively to conduct secure e-business over the Internet.

The PKI assumes the use of *public key cryptography*, which is the most common method on the Internet for authentication of a message sender or encryption of a message. Traditional cryptography involves the creation and sharing of a secret key for the encryption and decryption of messages. This secret key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the PKI is the preferred approach on the Internet. A PKI consists of

- A certificate authority that issues and verifies digital certificates
- A registration authority that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
- One or more directories where the certificates (with their public keys) are held
- A certificate management system

PKI is complicated but is a sound solution to a difficult problem, namely enabling two parties to exchange data securely over an insecure medium without the benefit of prior communication. It has been adopted by the popular Web browsers and is widely used for one-off business-to-customer (B2C) transactions. In general, however, PKI still faces challenges in terms of application support, interoperability between vendors, differing government legislation, and practical key management.

Large-scale PKI implementations therefore demand careful planning and management if goals are to be realized within the desired timescales. Where possible, companies developing these large-scale implementations for the first time should pilot the solution on an isolated, noncritical area of the business and always be realistic about what they hope to achieve.

WIRELESS NETWORK SECURITY SYSTEMS

It's an epidemic waiting to happen to many security experts. While most IT managers today have their hands full securing wired networks, their companies have been spending billions of dollars on wireless. Businesses will have spent $60 billion on wireless communications services and wireless network security by the end of 2005. This also includes 70% of the U.S. work force using some sort of wireless device, including cell phones, pagers, and mobile computing devices. That's good news for employee productivity, but bad news for companies ill-prepared to head off wireless network security breaches and debilitating viruses.

The only reason the wireless viruses of today have not been more damaging is that there's a lack of functionality and a lack of mature infrastructure globally. That's about to change. Industry analysts predict dramatic increases in wireless handheld use and the proliferation of new mobile capabilities. They expect to see 3.7 billion handsets, personal digital assistants (PDAs), and Internet appliances equipped with wireless capabilities by the end of 2006. With that, you get a full-scale epidemic in the works. Simply put, "It's coming."

The wireless world, with its often-incompatible alphabet soup of standards, may be new territory for many IT managers. Many enterprises have felt that protecting their wireless processes against viruses is one piece of the complicated puzzle they can afford to omit. They'll soon need to think again or face threats that could wreak havoc.

The good news is wireless network security vendors (even giants like IBM) are busy developing products to fight the viruses and security breaches of the future. Among them are those that head off problems on a wireless network level, within applications and on devices.

Overview of Wireless Network Security

To date, most wireless attacks have happened outside the U.S., in markets where wireless devices are more widely used. Nevertheless, one virus that did hit U.S. handhelds was known as the liberty virus. Some PDA users received what they thought was a program that would allow them to play a certain game for free, but when they double-clicked on the link, it launched a virus that erased all the data on the devices. The virus wasn't devastating for people who regularly back up their PDA information on their PCs. Nevertheless, more serious problems have occurred overseas in the form of viruses and malicious code that forced phones to dial particular numbers, intercepted transmissions, and stole data. One virus was distributed in Scandinavia as a short message. The virus rendered the buttons useless when a user received the message. In order to get their phones fixed, users had to take them in to their service providers.

New types of malicious code have been written that force wireless devices to make phone calls, because many of them also have telephony capabilities. One incident in Japan caught the attention of wireless operators and software companies around the globe. Users of NTT DoCoMo's (*http://www.nttdocomo.com/*) popular I-mode service received an email with what looked like an embedded Web site link. When customers clicked on the link, their phones automatically dialed Japan's emergency response number. Luckily, they could stop it before it got too bad, but such code could shut down a 911 system and have serious consequences. For example, similar viruses could be unleashed that might flood a company's call center or cause phones to dial a 900 number. If a virus that spread to all its mobile workers racked up significant charges, a corporation could be seriously affected.

The threat of data theft, perhaps, is more alarming to businesses. In order to prevent the interception of information as it's being transmitted, all wireless transmission standards have security built in, but they're known to be fallible. The developers of standards such as the wireless application protocol (WAP) and the wireless LAN 802.11b standard have included encryption technology designed to head off the threat of "sniffing."

Because the wireless network is essentially everywhere, sniffing is an inherent problem in wireless. Sniffers must have access to physical parts of the network in order to break into the wired world. The problem is that with wireless, they don't even have to be in the network. They can be in a van outside with a transmitter.

The widely used wireless LAN standard, 802.11, came under fire recently when researchers at the University of California at Berkeley figured out how to crack its built-in encryption. Still, there is some hope, because developers addressed wireless network security from the start and are working to beef it up before wireless LANs become more pervasive. Companies will also have to secure wireless transactions. There will be attacks on the devices themselves, but they quickly will be focused on transactions.

As devices develop more capabilities, these threats are expected to grow more serious and frequent. Typically, you should look to the past to predict the future. Every time there is a technology advancement, along with it comes new possible threats. Each time software companies release popular technologies in the PC environment, people use them to write malicious code. The same is expected with regard to wireless. For example, a Windows program can currently run on a Windows Compact Edition (CE) device, but CE doesn't yet support macros. Thus, the ability for viruses to spread is nil, because the device doesn't support macros.

Wireless devices are rapidly developing other capabilities. In the beginning the PDA was just something used to store contacts, but today they are little computing devices. There's more of a chance of things being used improperly as you create more functionality.

Most viruses have been regional so far, but the threat of viruses spreading around the globe grows as regions of the world begin to standardize wireless technologies. NTT DoCoMo, for example, opened its wireless network globally in 2003. Now, NTT DoCoMo threats can spread worldwide.

Also, the more capabilities supported by devices, the greater the potential for viruses to spread between PCs and mobile devices, which could enable viruses to spread very quickly. Windows CE will support Java script in the future so the same applications can run on PCs and handheld devices. Then viruses can spread easily via email or programs that synchronize PCs and handheld devices. Some wireless phones (including versions Nextel Communications sells primarily to businesses) already support a version of Java.

Thus, as 802.11 networks proliferate and mature, robust wireless network security solutions are required. The basic 802.11 wireless network security solutions that are available "out of the box" (service set identifier [SSID], MAC address filtering, and wired equivalent privacy [WEP]) are suitable for small, tightly managed wireless networks with low-to-medium security requirements. For wireless networks with high security requirements, the weaknesses in WEP encryption require a more robust solution. In addition, the manual task of maintaining MAC addresses and WEP keys becomes overwhelming as the number of wireless network clients increase. For larger wireless networks, or for networks with high security requirements, a VPN solution based on currently available technology provides a very scalable solution for 802.11 wireless networks. VPN for wireless is also a logical extension of the remote access VPN capability found in most large businesses today. On the horizon is 802.1X, a standards-based solution for port-level authentication for any wired or wireless Ethernet client system.

In addition, although distributed denial-of-service (DDoS) attacks have been recognized as a serious problem, there hasn't been any other attempt to introduce formal classification into the DDoS attack mechanisms. The reason might lie in the use of fairly simple attack tools that have dominated most DDoS incidents. Those tools perform full-force flooding attacks, using several types of packets. As defense mechanisms are deployed to counter these simple attacks, they are expected to be faced with more complex strategies.

The Computer Emergency Response Team (CERT) Coordination Center is currently undertaking the initiative to devise a comprehensive classification of computer incidents as part of the design of common incident data format and exchange procedures. Unfortunately, their results are not yet available. Thus, as of this writing, there have been no attempts to formally classify DDoS defense systems, although similar works exist in the field of intrusion detection systems.

Nevertheless, DDoS attacks are a complex and serious problem, and consequently, numerous approaches have been proposed to counter them. The multitude of current attack and defense mechanisms obscures the global view of the DDoS problem. This chapter is a first attempt to cut through the obscurity and achieve a clear view of the problem and its solutions. The classifications described here are intended to help the wireless network community think about the threats they face and the information warfare (IW) measures they can use to counter those threats.

One benefit of the development of DDoS classifications has been to foster easier cooperation among researchers on DDoS defense mechanisms. Attackers cooperate to exchange attack code and information about vulnerable machines and to organize their agents into coordinated wireless networks to achieve immense power and survivability. The Internet community must be equally cooperative to counter this threat. Good classifications for DDoS attack and defense mechanisms will facilitate communications and offer the community a common language to discuss their solutions. They will also clarify how different mechanisms are likely to work in concert and identify areas of remaining weakness that require additional mechanisms. Similarly, the research community needs to develop common metrics and benchmarks to evaluate the efficacy of DDoS defense mechanisms, and good classifications can be helpful in shaping these tasks, as well.

The preceding classifications are not necessarily complete or all-encompassing. We should not be deceived by the simplicity of the current attacks; for the attackers this simplicity arises more from convenience than necessity. As defense mechanisms are deployed to counter simple attacks, we are likely to see more complex attack scenarios. Many more attack possibilities exist and must be addressed before we can completely handle the DDoS threat, and some of them are likely to be outside the current boundaries of the classifications presented here. Thus, these classifications are likely to require expansion and refinement as new threats and defense mechanisms are discovered.

Finally, the DDoS attack classification and DDoS defense classification outlined in this chapter are useful to the extent that they clarify your thinking and guide you to more effective solutions to the problem of DDoS. The ultimate value of the wireless network security technology described in this section will thus be in the degree of discussion for the next computer forensics system, known as satellite encryption security systems.

SATELLITE ENCRYPTION SECURITY SYSTEMS

The boom in satellite communications is changing the way we work and live, but it is becoming a security nightmare for those organizations and governments whose survival depends on the protection of intellectual property distribution, electronic commerce, electronic battlefields and national security. The ability to securely exchange information between billions of users around the globe involving perhaps trillions of transactions is vital to the continued growth and usefulness of satellite communications as well as the Internet and intranets. Encryption—especially several layers of encryption on top of compressed data that is to be transmitted (via a highly directional microwave radio signal) to a satellite (uplink) from Earth and then transmitted down to Earth (downlink) and decrypted—can effectively solve the Internet's confidentiality and authentication problems.

This section shows how governments and organizations around the world can use satellite encryption to help preserve vital national secrets, limit attacks on a nation's information infrastructure, and eliminate security and authentication obstacles to electronic commerce. Specifically, this part of the chapter provides a brief overview of current satellite encryption technology, the threat from the Internet, encrypted satellite data transmitting (downlink) and receiving (uplink), and encryption cracking.

Current and Future Satellite Technology

A look at the potential threat to these orbiting systems from the Internet is of the utmost importance before covering how to use encryption to best protect them. As it stands today, the Internet is not secure, so the only option is to understand how attacks occur and how best to protect against them.

High-Tech Mayhem

Attacks on satellite systems regularly fill plot lines of Hollywood movies. For instance, in the James Bond thriller *Tomorrow Never Dies* terrorists steal an encryption decoder from the CIA and use it to transmit false longitude and latitude coordinates from a U.S. military satellite to a U.S. ship carrying nuclear missiles to make it appear that it is in international waters when the ship is actually within Chinese waters, resulting in the imminent threat of World War III.

Such incidents could be all too real in the near future. That's because as satellite-connected networked computers expand their control over world governments, the military, energy, power, water, finance, communications, and emergency systems, the possibility of electronic attack and catastrophic terrorism becomes increasingly possible. A serious threat is sure to evolve if the international community doesn't take steps now to protect these systems in the future.

High-Tech Highwaymen

Today's electronic highway is threatened by a new breed of *highwaymen*, called crackers, ranging from malicious pranksters to hardened terrorists. For the sake of public trust in the Internet, an infrastructure must be designed to support the safe use of land-based communication links or ground stations (called gateways, they connect terrestrial networks with satellite systems) as shown in Figure 3.5. Systematic mechanisms and protocols must be developed to prevent breaches of security while transmitting data to (uplink) a satellite or receiving (downlink) data from it.

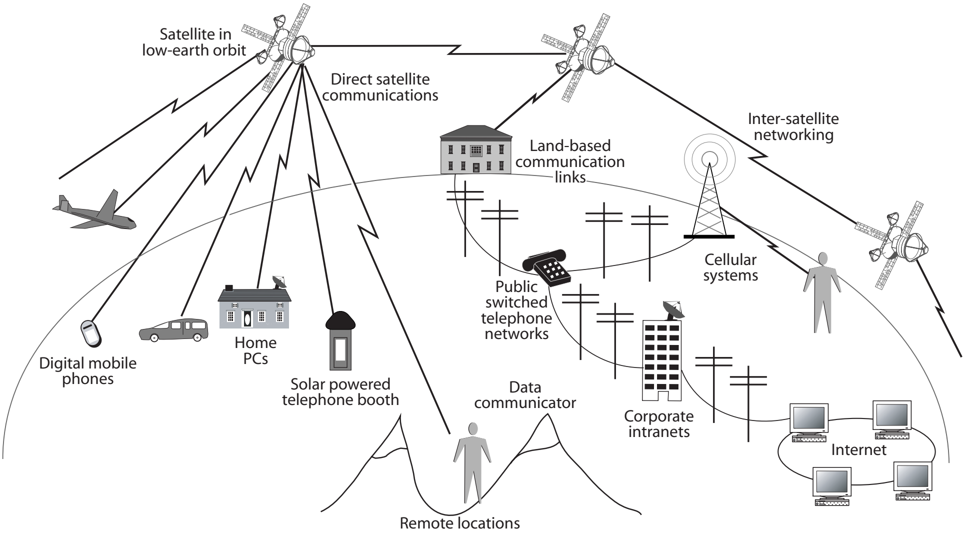

Satellite in low-earth orbit
Direct satellite communications
Land-based communication links
Inter-satellite networking
Cellular systems
Public switched telephone networks
Digital mobile phones
Home PCs
Solar powered telephone booth
Data communicator
Corporate intranets
Internet
Remote locations

FIGURE 3.5 The low Earth orbit (LEO) network.

Prevention versus Detection

Among the protection mechanisms are encryption for safeguarding the transmission of sensitive data (such as credit card numbers) to and from satellites, authentication by a password, and access controls such as permission to access files. All of these protection mechanisms are designed to ensure that only an authorized person can gain access to systems and alter information. Audit mechanisms are investigative tools that detect and quantify malicious behavior. For instance, some tools check the records (called *audit logs*) of system behavior, while others examine user activities on the system as they occur.

Odd Person Out Attacks

Suppose that an attacker is competing with Lisa for Jeremiah's business and wants to intercept Lisa and Jeremiah's email billet-doux. If the messages traveling over the Internet via satellite connection can be modified en route, the message Jeremiah receives need not be the one Lisa sent. To do this, the attacker must change the router tables so that all email messages between Lisa's and Jeremiah's computers are forwarded to some intermediate satellite system to which the attacker has easy access. The attacker can then read the messages on this intermediate satellite site, change their contents, and forward them to the original destination as if the intermediate site were legitimately on the message's path—a so-called *odd person out* attack.

Using encryption to hide the contents of messages, while often seen as the ultimate answer to this problem, is merely part of the solution because of a simple yet

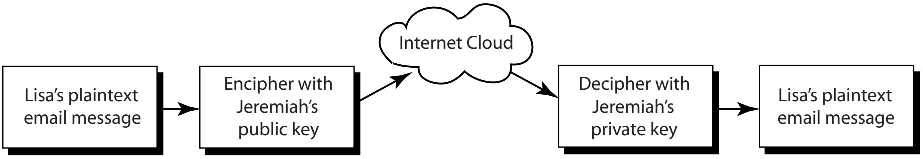

Internet Cloud
Lisa's plaintext email message
Encipher with Jeremiah's public key
Decipher with Jeremiah's private key
Lisa's plaintext email message

FIGURE 3.6 The path of a public-key-encrypted message.

fundamental problem of trust: how do you distribute encrypted keys? Public-key encryption systems provide each user with both a private key known only to that user and a public key that the user can distribute widely. With this scheme, if Lisa wants to send Jeremiah confidential mail, she enciphers a message using Jeremiah's public key and sends the enciphered message to him as shown in Figure 3.6. Only Jeremiah, with his private key, can decipher this message; without that key, the attacker cannot read or change Lisa's message.

Suppose the attacker is able to fool Lisa into believing that the attacker's public key is Jeremiah's, say by intercepting the unencoded email message that Jeremiah sent giving Lisa the public key and substituting his own. Thus, Lisa would encipher the message using the attacker's public key and send that message to Jeremiah. The attacker intercepts the message, deciphers it, alters it, and re-encrypts it using Jeremiah's real public key. Jeremiah receives the altered message, deciphers it, and the business deal goes sour.

The situation becomes even more complicated with the World Wide Web. Suppose Lisa uses a Web browser to view a Web site in Italy. The Italian Web page, put up by an attacker, has a link on it that says, "Click here to view a graphic image." When she clicks on the link, an applet that scans her system for personal information (such as a credit card number) and invisibly emails it to the attacker is downloaded along with the image. Here, Lisa trusted the implied promise of the Web page that only an image would be downloaded. This trust in implied situations (*this program only does what it says it does*) is violated by computer programs containing viruses and trojan horses. PC users spread viruses by trusting that new programs do only what they are documented to do and have not been altered, so they fail to take necessary precautions.

The ability to securely exchange information between two users or between a service provider and a user via satellite connection is vital to the continued growth and usefulness of satellite communications as we approach the next millennium. How can we use encryption to best protect these systems?

Satellite Encryption Secure Exchange

For the sake of public trust in the Internet, an infrastructure must be designed to support the safe use of land-based communication links or ground stations (gateways) as shown in Figure 3.5. An *encryption* infrastructure can be effectively designed to solve most of the confidentiality and authentication concerns of satellite transmission with the Internet. However, secure exchange can be either a one-way or a two-way encounter, and the satellite encryption requirements and strategies are quite different for each.

A one-way transaction is typified by email transmissions to and from satellites over the Internet. Although email messages are frequently answered, each message transmission is a unique, stand-alone event. A message sender may want assurance that the message can only be read by the intended recipient (confidentiality); a recipient may want assurance that the message came from the alleged sender without being altered en route (authenticity).

Client/server applications, Web exchanges, and many other online applications typify the second class of satellite communications and Internet exchange: two-way transactions. A two-way transaction first involves some sort of a logon function, in which a user connects to a service, and then an exchange of information between the user and the service occurs. For these two-way transactions, there are again two main security concerns: first, the service wants assurance that the user is not an impostor but actually the person claimed (authenticity). Then, once the service has accepted a user as legitimate and authorized, both the user and the service may wish to ensure that all information exchange between them is safe from eavesdropping (confidentiality).

Although these concerns seem similar, the solutions are quite different. Although many cryptographic tools can provide satellite communications and Internet security services, the best way to learn how they work is to look at two representative packages: PGP and Kerberos. PGP is a widely used email security package for one-way transactions, while Kerberos is a widely used client/server security package for two-way transactions. Between them, they incorporate the key cryptographic techniques used for Internet and satellite communications.

Pretty Good Privacy

PGP uses the RSA (Rivest, Shamir, Adelman) public key encryption scheme and the MD5 (Message Digest 5) one-way hash function to form a digital signature, which assures the recipient that an incoming satellite transmission or message is authentic—that it not only comes from the alleged sender but also has not been altered. The sequence for this is as follows:

1. The sender creates a private message.
2. MD5 generates a 128-bit hash code of the message.
3. The hash code is encrypted with RSA using the sender's private key, and the result is attached to the message.
4. The receiver uses RSA with the sender's public key to decrypt and recover the hash code.

5. The receiver generates a new hash code for the message and compares it to the decrypted hash code. If the two match, the message is accepted as authentic.

The combination of MD5 and RSA provides an effective digital-signature scheme. Because of the strength of RSA, the recipient is assured that only the possessor of the matching private key can generate the signature. Because of the strength of MD5, the recipient is also assured that no one else could have generated a new message that matched the hash code and, hence, the signature of the original message.

PGP also solves the confidentiality problem by encrypting messages to be transmitted via satellite or to be stored locally as files. In both cases, PGP uses the confidential IDEA (international data encryption algorithm) encryption algorithm. IDEA is a relatively new algorithm that is considered to be much stronger than the widely used date encryption standard (DES).

In any conventional satellite encryption system, one must address the problem of key distribution. In PGP, each conventional key is used only once. That is, a new key is generated as a random 128-bit number for each message. This session key is bound to the message and transmitted with it as follows:

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only.
2. The message is encrypted, using IDEA with the session key.
3. The session key is encrypted with RSA using the recipient's public key and is prepended (to prefix a string or statement with another or to place a word or set of numbers in front of an existing word or set of numbers; for example, to prepend "sub" to "net" would yield "subnet") to the message.
4. The receiver uses RSA with its private key to decrypt and recover the session key.
5. The session key is used to decrypt the message.

Many people underestimate the difficulty of key distribution in a public key encryption scheme. The common misconception holds that each user simply keeps his or her private key private and publishes the corresponding public key. Unfortunately, life is not this simple.

An impostor can generate a public and private key pair and disseminate the public key as if it belonged to someone else. For example, suppose Ellen wishes to send a secure message to Shawn. Meanwhile, Mark has generated a public and private key pair, attached Shawn's name and an email address that Mark can access, and then published this key widely. Ellen picks this key up, uses it to prepare her message for Shawn, and then uses the attached email address to send the message. The result is that Mark receives and can decrypt the message, Shawn never receives the message, and, even if he did, he could not read it without the required private key.

The basic tool that permits widespread use of PGP is the public key certificate. The essential elements of a public key certificate are the public key itself, a user ID consisting of the key owner's name and email address, and one or more digital signatures for the public key and user ID.

The signer in effect testifies that the user ID associated with the public key is valid. The digital signature is formed using the private key of the signer. Then, anyone in possession of the corresponding public key can verify the validity of the signature. If any change is made to either the public key or the user ID, the signature will no longer compute as valid.

Certificates are used in a number of security applications that require the use of public key cryptography. In fact, it is the public key certificate that makes distributed security applications using public keys practical.

As the need for security on the Internet and satellite transmissions increases, new mechanisms and protocols are being developed and deployed, but a system's security will always be a function of the organization that controls the system. Whether the Internet or satellite communications become more secure depends entirely upon the vendors who sell the systems and the organizations that buy them.

Ultimately, people will decide what and how much to trust, so satellite communications security is a nontechnical, people problem, deriving its strength from the understanding by specifiers, designers, implementers, configurers, and users of what and how far to trust. To begin addressing this challenge, IT managers need to

- Get to know the key emerging vendors in this field
- Begin learning about how public key cryptography is being woven into the *soft* infrastructure of the Internet and satellite communications—and by extension, into intranets as well
- Prepare to respond to business requirements for detailed, real-time measurement and reporting of document usage within the organization, as well as the use by outsiders of documents created within the organization
- Spend quality time with business unit managers, educating them on these new technologies and brainstorming applications that make use of them

This section provided a brief overview of the current satellite encryption policies, the threat from the Internet, encrypted satellite data transmitting (downlink) and receiving (uplink), and encryption cracking. Now let's go on to the next computer forensics system: instant messaging (IM) security systems.

INSTANT MESSAGING (IM) SECURITY SYSTEMS

The security threats from IM are straightforward. Since deployment isn't controlled, the enterprise can't keep a rein on how the systems are used. With the public IM networks, the individual employee registers for service. If the employee leaves a company, the firm has no (technology-based) way to prevent him from continuing to use the account, or from continuing to represent himself as still working for the company. Furthermore, without additional tools, the company has no way of archiving IM messages for legal or regulatory purposes, or of monitoring and controlling the content of messages to filter for inappropriate communications.

There are the obvious holes that IM opens up on the corporate network. Each of the IM networks uses a well-known port that must either be left open on the corporate firewall to allow traffic in or closed, which, at least in theory, bans that service to end users.

Securing IM

Certainly the latter option has some appeal: 34% of all companies simply block all IM traffic according to industry analysts. One downside to this strategy is that because workers find IM useful, blocking it isn't popular or necessarily even a good business move.

Another downside is that blocking might not work. If the IM port has been blocked, all the popular clients today are designed to fall back to port 80, the Web port, and that's usually open. The administrator would have to block individual URLs for the IM services to keep traffic from coming through port 80.

Given IM's pervasiveness, enterprises can't think about security in a vacuum; it has to be part of a larger management structure. Policies may regulate what types of files can and can't be transferred via IM systems to limit the potential for introduction of viruses; some may even do virus scanning. Products also can examine message content much like existing email spam filters.

Thus, IM management and security systems act as proxies for IM traffic going into the network, which imposes policies before letting traffic through. Besides addressing security, this architecture puts the IM management and security vendors in a position to deal with the pesky problem of the lack of interoperability among networks.

So, you'd think IM would be hot, but even the vendors that have made their name in IM are trying to expand their focus to other real-time applications such as voice over IP and conferencing. Vendor representatives are surprisingly open about their reasons: IM as a stand-alone application gets commoditized pretty quickly.

Indeed, the tough thing about IM security and management isn't that it's technically hard to do; it's that adoption is happening so quickly that network managers are playing catch-up.

NET PRIVACY SYSTEMS

The philosophical focus of a privacy management perspective is geared toward the improvement of the bottom line for private companies and cost control and resource optimization for nonprofit and government organizations. All types of organizations need to develop privacy policies that maximize the benefit of reusing information in as many ways as possible while minimizing the risks associated with potential privacy violations. Although this balance is essential in an information intensive world, it is clear that it is not going to be easy for organizations to achieve the balance between privacy and the optimization of resources.

Privacy is a social, political, and economic issue. Privacy protection for the individual was born with democracy and was originally designed to keep oppressive governments from intruding on individual freedoms. In a world of advanced industrial societies where most major countries are at peace with each other, the violation of privacy and civil liberties has come under new threats. People still have every reason to keep a tight reign on snoopy governments (like the use of the Patriot Act), but now they must also be concerned about the commercial violation of individual privacy rights and desires.

Some private companies have made a business out of selling information about individuals, groups, and organizations. This has raised considerable concern among privacy advocates. Information brokers are only part of the commercial privacy violation equation. Most for-profit companies, government agencies at all levels, and even nonprofit organizations collect large amounts of information about the people they serve or seek to serve. How this information is used and protected has become a concern, and assuring the privacy of such information has turned into a new management challenge.

Managing Privacy Is the Business Challenge of the 21st Century

Protecting the privacy of enterprise information, data on customers, and corporate trade secrets has become a major concern for managers in all types and sizes of organizations. Laws are often ambiguous, social thought toward privacy is volatile, emerging technologies present new and complex challenges, and political winds are blowing hard from many directions. Surviving the chaos surrounding information privacy requires a comprehensive company-wide privacy plan.

There is considerable debate in the U.S. as well as most industrial countries on how to deal with privacy issues. It is not likely that this debate will end anytime soon. Also uncertain are the direction of the debate and possible outcomes that will impact legal and social requirements that enterprises will have to meet to protect information privacy. The Internet has compounded the difficulties enterprises face in managing privacy efforts. These difficulties will increase as more people around the world use the Internet. Industry analysts project that by 2008, there will be approximately one billion Internet users worldwide.

The Internet has contributed to people's awareness of privacy issues in four ways. First, the Internet has resulted in a huge increase in the number of people using computers to seek information and make purchases. Second, there have been several incidents that have resulted in considerable and less than favorable press coverage for enterprises that have suffered from privacy problems. Notably, in late 1999 and early 2000, Web technology that tracks how people use the Internet came under fire. Third, many organizations had their first experiences in dealing with large-scale privacy issues. They range from small new Web-based companies to large enterprises that started using the Internet for marketing, sales, or information dissemination. Fourth, the global nature of the Internet has presented new challenges to governments and enterprises. The combination of these trends sets the stage for potential privacy conflicts.

In many ways, privacy issues can be viewed as a clash of cultures. The global nature of technology usage and thus international information exchanges, whether they are voluntary, a result of technology architectures, or stem from out-and-out deception, puts governments and international organizations in adversarial positions. The desire of new Web-based companies to build a viable enterprise by capitalizing on information to develop marketing and sales approaches or even just collecting information using Internet technology for the purpose of selling it, throws the entrepreneur into conflict with governments, consumer groups, and private individuals.

Beyond the commercial use of the Internet, global competition has contributed to a wave of industrial spying and the theft of trade secrets. The desire of companies, and in some cases governments, to make their enterprises or societies more competitive has resulted in numerous cases of international information theft. The Internet plays a role in this process by enabling people to move information around the world faster and to provide low cost communications methods for information theft rings. The Internet can also provide a gateway into corporate information systems that hackers and information thieves can exploit to gain access to customer data, trade secrets, or corporate processes.

In the information-intensive environment of the 21st century, politics is of course a factor. In the U.S. everything can become political fodder. The Internet, privacy, and consumer rights have historically been separate issues, but the dynamics of capitalism and cultural conflicts over privacy have fired rhetoric from Washington, D.C. to San Francisco to Manila to Stockholm and around the world. These issues make for great debates, at least on Sunday morning talk shows. These issues also become content for the plethora of television news shows and pop culture news magazines. American politicians know their drills well. Politicians know they must promise goodness, salvation, and protection of the family, community, and country. What politicians do not know is how to address the complex issues of privacy in a world connected by the Internet that is laden with greed and corruption and has hundreds of millions of relatively naive people blindly surfing into situations in which their privacy can be readily compromised.

In addition to their ineptness in the face of complex issues, politicians have a fear of going against major trends. This is the age of the Internet boom. To be politically correct one must agree that this is a great revolution and that it is something that will make economies stronger and the world a better place. Of course, it is also good politics to protect children from predators and old people from rip-off artists. The issue of protecting children and their privacy on the Internet has become a permanent part of the political process. The inevitability of the child protection issue is fueled by an increasing number of children using the Internet. According to industry analysts, by 2008 there will be over 130 million people under the age of 18 using the Internet. Politicians love such meaty issues, and the protection of 130 million children is one that they will not be able to resist.

On the other hand, politicians prefer to avoid issues that are complex or that require them to apply critical analysis to develop long-term solutions to major societal problems. It is unfortunate that when politicians try to deal with complex issues they usually make a mess of things. This was painfully demonstrated by the passage of the Communications Decency Act (CDA), which was rapidly ruled unconstitutional by the U.S. District Court. Congress does not know how to deal with the issue of privacy, and it is likely that any effort they put forth will be at least as messy as the CDA. Another example of quickly shifting government positions is the Federal Trade Commission (FTC) first being reluctant to push for greater privacy protection and then in late spring of 2000 making an about face and taking the position that Congress should pass new legislation.

Implementing an Enterprise-Wide Privacy Plan in a Chaotic World

It is expected that the chaos surrounding privacy issues will continue. For that reason, having a comprehensive corporate privacy plan is of the utmost importance. Business managers must develop and implement an enterprise-wide privacy plan. This is important because organizations are becoming more dependent on information systems to manage critical financial data as well as customer records and product data. It is also important because of increasing regulatory and social pressures concerning the protection of individual privacy and proprietary corporate information.

This author's position on privacy is very straightforward. Enterprises need to avoid potentially costly lawsuits and embarrassing public relations incidents that may result from revealing information that is protected by law, that management has determined could be detrimental to the enterprise if known by competitors or the public, or that customers feel should be kept private.

Also, this author's view of privacy management is that it needs to be comprehensive and enterprise-wide. Thus, to develop a solid privacy plan all departments and functions within the company need to be involved. This includes but is not limited to the IT department, legal counsel, customer relations, public relations, product development, manufacturing, and the accounting or financial management department. In order to successfully implement a privacy plan all departments need to understand the plan and corporate policies and procedures regarding the protection of privacy. In addition, the implementation and effectiveness of the privacy plan needs to be evaluated on an ongoing basis.

The goal here is to provide you with a process to manage privacy in your enterprise. This is done by giving you basic building blocks to understand the process of developing, implementing, and monitoring privacy plans, policies, and procedures. With that in mind, let's move on to the next computer forensics system: ID management security systems.

IDENTITY MANAGEMENT SECURITY SYSTEMS

Identity management is the creation, management, and use of online, or digital, identities. Hundreds of millions of people around the world now use the Internet daily at home and at work, facing a multiplicity of corporate applications and e-business interfaces. Many such applications and interfaces require a unique user name, and as a result, an individual typically possesses not one but several digital identities.

Additionally, digital identities are not perpetual: they are created for new employees, and when those employees leave, their digital identity expires (or should expire) as of their termination date. An employee moving from one part of an organization to another—or being promoted to a higher management level—may need to have updated access rights and other information attached to his or her digital identity. Identity management is therefore also about being able to manage the full life cycle of a digital identity from creation and maintenance to termination, as well as enforce organizational policies regarding access to electronic resources. It is not simply the ability to store or provision digital identities. While these are critical capabilities, they are just two components of an overall solution.

Ultimately, identity management will help organizations do business and get things done. By authenticating and authorizing digital identities, an identity management system will improve administrative productivity while keeping enterprise resources secure, as well as streamline e-business transactions. Users will enjoy a more convenient experience, and organizations will benefit from more efficient processes and expanded business opportunities.

In the absence of identity management, the staggering proliferation of identities on the Internet—and the challenge of managing them securely and conveniently—

is threatening to inhibit the growth of e-business. Identity management will help organizations control access to enterprise systems and resources, facilitate efficient and secure collaboration and commerce with business partners, and provide the level of trust, convenience, and reliability needed to grow e-business revenues and enhance profitability. In addition, an effective identity management solution will reduce the number of unique user identities, enable identities to transcend the online boundaries of a single business, and include secure systems to create and manage those identities.

The Challenges of Managing Digital Identities

The recent convergence of three events has created a sense of urgency around identity management. They will be discussed briefly, and then we will detail some of the critical user concerns and business issues that must be addressed by any identity management system.

Aggregation

There is an incalculable amount of content on the Internet. To help business and home users find the sites and services they want, corporate portals and content aggregators like Yahoo emerged.

In the process of providing more content and services, these aggregators have developed relationships with users—including capturing their online identities. When a user accesses content and services through these aggregators, his or her digital identity is captured. In an enterprise environment, this provides valuable tracking of information; for Web sites, each captured identity is an asset they can leverage for their own—and their business partners'—marketing purposes.

Web Services

Web services are modular applications that enable the transformation from a software purchasing and physical ownership model to a software subscription or "rental" model with remote execution. Examples of Web services currently prevalent on the Internet include calendaring, supply chain management, customer relationship management, order fulfillment, sales force automation, music on demand, and instant messaging. Businesses reduce IT costs with this zero-footprint approach to software deployment. Consumers find Web services convenient and cost-effective because they don't need to go to a physical store and then purchase and install software, and updates can be downloaded from the Internet. Software companies appreciate Web services because they save packaging, inventory, and distribution costs.

However, it is a significant challenge to verify a user's identity and mitigate the risk associated with providing high-value or sensitive services in an online business-to-business (B2B) or business-to-consumer (B2C) environment. Also, there are different levels of trust. A company can trust an employee's identity more than that of an external partner or customer because the company has more control over the provisioning and maintenance of the employee's identity. An identity management solution provides that trust as it confirms that a user is authenticated and authorized to access applications and services.

Online Partnerships

Many businesses are forging online partnerships with organizations that offer complementary services, both internally (to improve productivity) and externally (to expand their customer reach). An example of the former would be a company's human resources department that allows its health plan and 401(k) vendors to cross-market value-added services on the company's intranet site. A B2C example would be an airline that enables customers who have already logged in to its Web site to access hotel, rental car, and other services online. This would be convenient for customers and benefit the individual companies by driving traffic to their Web sites.

User Concerns and Business Issues

Beyond these three convergent events, there exist real concerns among the two audiences that would ultimately benefit from an identity management system: users (employees, partners, and customers) and e-businesses. It is critical, therefore, to understand their issues and to design a solution they will embrace. The challenges that exist are making enterprise resources costly to manage and vulnerable to attack and are impeding the growth of e-business because they create fear in consumers and constrain the ability of businesses to operationalize their business models.

First, let's explore user concerns. Recently, industry analysts conducted a study in which users were asked what they found most bothersome about the Internet. Their answers fell into three categories: security, convenience, and privacy. These three issues are relevant to both consumer and business users, relate very strongly to identity, and must be paramount in the design of any identity management system.

Security

According to the FTC, there were 108,000 cases of identity fraud in the U.S. in 2003, including both electronic and real-world cases. The two most prevalent targets of fraud were both Internet-based: online auctions and Internet service provider (ISPs). Many online identity thefts are related to fraudulent credit card use made possible by unauthorized access to customer databases, but they can also occur in enterprise settings; all it takes is an unoccupied computer and the time needed to crack a password.

Identity fraud (which will be discussed in detail later in the chapter) affects users negatively in both home and work environments. When a consumer's digital identity is stolen, the thief often has access to credit card numbers and can run up huge bills for which the victim is responsible. On the enterprise side, if someone uses another identity to obtain and release proprietary information, that usage could be tracked and the innocent employee could be blamed—and probably fired—for something he or she didn't do. An identity management system can guard against identity theft by standardizing and automating the provisioning, maintenance, and revocation of digital identities.

Convenience

The point of security systems is to make it extremely inconvenient for unauthorized users to gain access. To do that, however, many users with good will and honorable intentions have been required to remember numerous complex passwords—and because they invariably do not remember, high support and help desk costs due to forgotten passwords often result.

Mindful that consumer and business users want convenience, many Web browsers support password caching. This means that a user who has logged on to a particular Web site in the past can easily (and sometimes automatically) log on again without having to retype or even remember his or her password. Of course, this means that anyone who sits down at that person's computer can log on and illegally use an already authorized identity.

Clearly, a balance must be struck between convenience and security. If a single, shared online identity that eliminates the need for multiple registrations and passwords represents convenience in an identity management system, then that system must add strong security via authentication technologies (such as digital certificate-based smart cards, tokens, and biometrics) as well as fine-grained authorization through access management technologies. The goal is to make customers happy and employees and partners productive, while keeping the enterprise secure and efficient.

Privacy

A key benefit of an identity management system is that a single user identity can be used across multiple Web sites and electronic resources. This great convenience, however, can pose significant privacy issues. For one thing, it would be possible for someone to track which Web sites, applications, or databases a user had accessed, which could be interpreted as a violation of privacy. Second, the collected preferences and purchasing history from different Web sites linked to the same identity could result in unwanted electronic profiling and unauthorized surveillance of a user's Internet habits.

Any identity management system must adequately protect sensitive user information and adhere to the four key elements of a privacy policy:

Notice: Users receive prior notification of information practices.

Choice: Users are able to give specific consent to the gathering and use of information.

Access: Users have the ability to access their personal information.

Security: Users have assurance that the organization has taken and is taking measures to prevent unauthorized access to and use of personal information.

Business Issues: Trust, Control, and Accountability

In addition to these user concerns, there are three primary business issues that must be addressed by an identity management system: trust, control, and accountability. A single example illustrates how these issues arise in a common enterprise scenario.

Trust via Authentication

Consider an employee collaboratively developing a product in a virtual environment with a business partner. He or she will need access to internal resources, as well as controlled access to the collaborative environment and to specific partner resources. An identity management solution would enable the user to access these varied distributed resources with single sign-on convenience—but the system falls apart if the business partner can't trust the authentication process the original company used to approve its employee's credential. Strong authentication—in the form of tokens, smart cards, digital certificates, or even biometrics— provides the requisite trust in the user's digital identity.

Control via Access Management

Assuming the employee's digital identity is trusted, policies should be applied to control access to protected resources. A digital identity needs to have the proper access profile attached to it in order for the employee to gain access to the partner's resources. Enforcement, then, ensures the effectiveness of online business processes.

Accountability via Audit

As the employee moves from resource to resource, both internal and external, an audit trail must be kept of which resources are being accessed and what is being done with them to ensure that policies are being honored and enforced. The employer and the business partner need to share this information to hold all parties accountable for the integrity of the system and the success of their partnership.

These issues are significant because companies historically have been reluctant to share customer and employee information with other organizations. Also, companies have been advised to perform their own vetting and authentication on customers and not rely on someone else's prior approval. These are cultural and business process issues that technology alone may not be able to address but that must be considered within the larger framework of policies and regulations around which an identity management system is built.

Approaches to Identity Management

To date, there have been three distinct approaches to developing an identity management system, each appropriate to different circumstances and requirements. Each also has its pros and cons. As presented, they represent a conceptual and technological evolution from one-on-one and closed systems to more universal approaches that seek to address the wide range of issues that have been discussed thus far. Respectively, these approaches are known as silo, closed community, and federated.

Silo

In a silo model, each business creates a unique relationship with its customers, employees, and partners through Internet, intranet, and extranet sites, respectively. The silo approach is the most prevalent today because it is simple to implement, allows a business to maintain complete control of its users' identities and preferences, provides uncontested branding and messaging to users, and limits security and privacy risks.

The silo approach also has some significant drawbacks. Users are inconvenienced when they have to interact with numerous silos (even within a single organization), each requiring individual log-on processes and passwords. For businesses, the silo model inhibits cross-selling opportunities; it is also expensive to maintain—and burdensome to administer—multiple silos.

Closed Community

A closed community is one in which a central business unit defines and brokers trust to all member organizations in the community. An example would be any group of companies, government agencies, or educational institutions that have banded together to serve a common user group or to establish an online B2B exchange. From any member Web site, a user can gain access to the Web sites of other partners.

If a user wants to visit the Web site of a company outside the closed community—say, a competitor of one of the members—he or she would have to go to that site separately. The advantages of a closed community approach are that it provides a reasonable degree of simplicity and control, can be economical for businesses when all agree to pool resources and create a central infrastructure, and offers the ability to delegate the creation and administration of user identities. The disadvantages are that users have a limited choice of companies to deal with and would be inconvenienced if they needed to belong to multiple communities or leave a community because a preferred vendor is not a member. Further, most businesses don't want to cede authority to a central entity, and there exists a single point of failure in a closed community that if compromised could undermine the entire infrastructure.

Federated

In a federated model, each partner agrees to trust user identities issued or authenticated by other organizations while maintaining control of the identity and preference information of its own users. A common example of a federated model is the passport: each country independently issues passports that are trusted by all the other countries.

The federated model promises consolidated authentication capabilities across distributed computing resources. Users can log on to a range of participating Web sites using a single email address and password. For businesses, benefits include greater efficiency and security; better services for employees, partners, and customers; and new revenue opportunities. The only drawback is that it requires businesses to cooperate, adhere to best operating practices, and develop a high level of trust.

Overall, it appears that the federated model is emerging as the preferred next step both for silo organizations looking to expand their reach and for closed communities seeking to connect with other communities on the Internet. Clearly, the design for federated identity will need to be attractive to both large and small organizations and offer the flexibility to adapt to existing identity management systems.

An identity management solution is about intelligently using the identities that have been created to do e-business. In addition to creating, managing, and revoking digital identities, it helps develop and enforce authentication and access management policies as well as provide the accountability required in e-business today. The vision of identity management, therefore, incorporates a broader definition, a technology-neutral approach to integration and a flexible architecture that enables interoperability with multiple identity systems inside and outside organizations. The components of an identity management environment should include the following:

Data store: The more user information that is collected, centrally stored and protected, the more layers of access and greater breadth of services an organization can provide to users.

User provisioning: Deploying digital identities and access rights based on business policies for employees, business partners, and customers must be done accurately and securely at the outset in order to reduce problems down the line. Assigning, maintaining, and revoking these identities and rights should be a centralized function.

Authentication policy management: Once someone steals a user's digital identity, the whole system becomes vulnerable. Authentication policies help ensure that organizations know who is using a digital identity, thus creating trust in the system.

Authorization policy management: Authorization policies are designed to ensure that only appropriate resources can be accessed by a given digital identity. This helps ensure that the right people get the resources and information they need, while enterprise systems are protected from unauthorized access.

Centralized audit: Organizations need to track what users are doing and make sure there are no blatant inconsistencies that indicate a problem. Having an audit trail of what digital identities are being used for holds users accountable.

Integration: Putting the individual pieces together in a technology-neutral architecture enables sharing, ensures interoperability, and facilitates single sign-on capabilities. It also makes the system scalable, easy to administer, and quick to deploy. A single federated identity enables a user to be authenticated from all other partners in the model.

As more and more enterprise applications and resources get pushed onto the Internet—including a range of Web services that organizations deploy and procure for employees, partners, and customers—companies need to be able to trust the identities of users who seek to access them. Further, they need to manage and control authorized identities to ensure they are current and are being used in accordance with established policies.

For this reason, organizations need to assess their own identity management needs, engage in detailed discussions with business partners about their needs and plans, and explore with a reliable vendor how to implement and integrate such a solution in their IT environments. The challenges that have brought the issue of identity management to the fore will only grow and exacerbate the problems that have stunted the growth of e-business and contributed to information security breaches around the world.

An open standard for identity management—including authentication, single sign-on, and Web access management capabilities—will help organizations lower costs, accelerate commercial opportunities, and increase user productivity and customer satisfaction. A federated approach will bring substantial benefits to users and businesses alike. Users will appreciate

- The convenience of a single identity and authentication for a wide range of enterprise resources, applications, and Web sites
- The ability to specify under what conditions certain pieces of information can and cannot be shared
- Policies and standards on data storage, usage, and sharing designed to protect their privacy and prevent fraud and identity theft

Businesses will be able to

- Trust the digital identities of employees, partners, and customers
- Receive pre-authenticated users from business partners' sites
- Maintain their own user data
- Introduce new services and identify new business opportunities
- Reduce internal IT and system integration costs by embracing a technology-neutral solution that is interoperable with major identity systems

With the preceding in mind, the aim of the next section is to help you begin the process of guarding against and recovering from identity theft.

IDENTITY THEFT

Quite simply, identity theft is the appropriation of an individual's personal information in order to impersonate that person in a legal sense. Stealing someone's identity enables the thief to make a frightening number of financial and personal transactions in someone else's name, leaving the victim responsible for what may turn out to be mind-boggling turmoil in his or her life.

Identity theft is not new. It has been around for a long time. There was a time when an individual could flee his or her life, town, and mistakes and go somewhere far away pretending to be someone else—and, no one knew better. The ramifications of stealing someone's identity did not have the far-reaching implications that they do today for the person whose identity is stolen. Those were the days before credit reporting and high-tech methods of tracking and sharing information were commonplace.

Identity theft can still be done by such low-tech means as knowing someone else's basic identifying information and initiating personal transactions in that person's name, but today, identities can also be stolen using highly technical and sophisticated means of obtaining the personal data of a stranger. However it is done, whether the identity thief uses high- or low-tech means of getting your personal information, an individual can become someone else very easily. The difference today is that what an identity thief does as someone else reflects very quickly on the victim's reputation. An individual's life can be devastated by the loss of good name and the financial or personal mess that results.

Identity theft is always personal—after all, it is one's own identity that is stolen! Someone literally assumes your identity and leaves a damaging trail of credit card abuse and exposed personal information all over the Internet (to your creditors and possibly worse). Thieves could be roommates, relatives, friends, estranged spouses, or household workers—with ready access to their victims' personal papers.

Opportunistic Theft

The thief may be an opportunist—one who sees his chance and takes it. The thief's motive is to gain goods and services at someone else's expense.

Living Large on Your Good Name

The sad part is that it is next to impossible to stop a determined identity thief. Who is going to apprehend him? Occasionally law enforcement agencies, including the Secret Service, bust up identity theft crime rings that involve many victims and millions of dollars, but they don't chase down single crooks that commit *victimless* crimes.

Professional Criminals

Identity thieves may be professionals. This could be individual hackers out to get what they can or highly sophisticated crime rings that make a business out of fraud.

How Identity Theft Is Done

In the course of a normal day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, call home on your cell phone, order new checks, or apply for a credit card. You may do any of a hundred little things each of us does every day that involve someone knowing who we are. Chances are, you don't give these everyday transactions a second thought, but an identity thief does. Those who make a profession of stealing identities give it a great deal of thought, indeed.

Despite your best efforts to manage the flow of your personal information or to keep it to yourself, skilled identity thieves may use a variety of methods (low- and high-tech) to gain access to your data. The following are some of the ways imposters can get and use your personal information and take over your identity:

- They steal wallets and purses containing your identification and credit and bank cards.
- They steal your mail, including your bank and credit card statements, preapproved credit offers, telephone calling cards, and tax information.
- They complete a change of address form to divert your mail to another location.
- They rummage through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving."

- They fraudulently obtain your credit report by posing as a landlord, employer, or someone else who may have a legitimate need for (and a legal right to) the information.
- They get your business or personnel records at work.
- They find personal information in your home.
- They use personal information you share on the Internet.
- They buy your personal information from "inside" sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services, or credit.
- They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there's a problem.
- They open a new credit card account, using your name, date of birth, and social security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- They establish phone or wireless service in your name.
- They open a bank account in your name and write bad checks on that account.
- They file for bankruptcy under your name to avoid paying debts they've incurred under your name or to avoid eviction.
- They counterfeit checks or debit cards and drain your bank account.
- They buy cars by taking out auto loans in your name.

How Your Personal Information Can Be Used Against You

Once the thief has basic information about you, there are a number of ways it can be used. If the thief has *seen* your credit card, he or she now knows who issued it. It is then a simple matter to call the financial institution and request a change of mailing address. Now, the thief can run up charges on your account. You don't realize what's happening for a while because you haven't gotten a bill. By the time you wonder what has happened to your bill and call the credit card company, it is too late.

An identity thief who has enough information about you can open a new credit card account in your name. Using your personal data to get it approved, the thief has at least a month (and maybe more, depending on the policy of the lender) before the account is closed for lack of payment. The balance on *your* new account by that time could be devastating—not to mention that the late payments have been reported to the credit bureau.

Then there are the counterfeit phone services that the identity thief can open in your name with the right information. Huge long distance and service bills can be charged to you because now the identity thief is getting the bill—not you. The trouble is, the identity thief isn't paying the bill. The end result is the same as with a phony credit card—you are left with a monstrous bill and your delinquency is reported to the credit bureau.

If an identity thief is able to steal your checkbook, or through some illegal method, obtain new checks on your account, he or she may bleed your bank account dry before you know what's happened. In other words, an identity thief can hurt you by opening a bank account in your name, possibly with a cash advance from your bogus credit card, and then write bad checks against that account as often as possible before the bank reports *your* felonious conduct.

An identity thief with access to your personal data can take out loans in your name: house loans, car loans, boat loans, etc. If the thief is good enough, he or she gets the goods and you get the bill.

The ultimate dirty deed an identity thief may do is to file for bankruptcy under your name. This would prevent the thief from having to pay debts incurred in your name. If they've been living in a home or apartment as you, they might file for bankruptcy to avoid eviction. Never forget the thief who has a personal agenda to cause you harm—what could be better than bankruptcy?

These are just some of the ways that the theft of your identity can wreak havoc in your life, and thinking about them is enough to scare the daylights out of you. It definitely is enough to make a person start thinking about how to protect himself.

Once the thieves have some of your personal information, they can start applying for credit cards in your name—giving an address that is often different from yours. Sloppy credit-granting procedures give thieves plenty of opportunities. A lot of credit granters do not check records. They are more interested in new applicants than in verifying the authenticity of the applicants.

Identity thieves may buy a car or rent an apartment in your name. Some may even commit crimes in your name. For example, in one case, the impostor was a major drug dealer using the identity of a highly ranked corporate executive. When traveling overseas, the executive now has to carry an official letter that explains he is not the drug dealer. Still, cops recently broke into the man's house and into his bedroom with guns drawn. While this is an extreme case, many identity theft victims have been denied student loans, mortgages, credit accounts, and even jobs. Some have had their telephone service disconnected and their driver's licenses suspended or been harassed by collection agencies. So where can you get immediate help if your identity has been stolen?

Help for Victims of Identity Theft

The FTC collects complaints about identity theft from consumers who have been victimized. Although the FTC does not have the authority to bring criminal cases, they can help victims of identity theft by providing information to assist them in resolving the financial and other problems that can result from this crime. The FTC also refers victim complaints to other appropriate government agencies and private organizations for further action.

If you've been a victim of identity theft, file a complaint with the FTC by contacting their Identity Theft Hotline by telephone: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or online: *http://www.consumer.gov/idtheft.*

Other agencies and organizations also are working to combat identity theft. If specific institutions and companies are not responsive to your questions and complaints, you also may want to contact the government agencies with jurisdiction over those companies.

Getting Serious About Identity Theft

Victims of identity theft are finally getting some respect—or at least some long-deserved recognition. In 1998, when Congress made identity theft a federal crime, it directed the FTC to establish a clearinghouse for identity-theft complaints and assistance. That came on the heels of a General Accounting Office report documenting how widespread identity theft is becoming. The Secret Service, for example, says victims and institutions in its identity-fraud investigations lost $4.01 billion in 2003, up from $1.78 billion in 2000.

Limited Resources

The FTC maintainsa a database of complaints, referring them to law enforcement agencies at the state and federal levels. Consumers don't have to call the FTC and the Secret Service and the FBI. The FTC thinks identity theft is a significant, growing problem. Therefore, it is expected that there will be a significant increase in the number of federal prosecutions.

The feds typically focus on large-scale scams. That leaves many cases in the hands of local police. Most police departments don't have the resources to investigate many cases, as suspects are often unknown and located in other jurisdictions. All the police can do in most instances is file a police report, but that still helps.

BIOMETRIC SECURITY SYSTEMS

While a biometric is the actual characteristic or trait, a biometric system is the computer hardware and software used to recognize or verify an individual. Although there are many variations in how specific products and systems work, there are a number of common processing elements.

Collection

As a first step, a system must collect or "capture" the biometric to be used. One essential difference between the various techniques is the characteristic (body part or function) being analyzed. Obviously, this will influence the method of capture. All biometric systems have some sort of collection mechanism. This could be a reader or sensor upon which a person places his finger or hand, a camera that takes a picture of his face or eye, or software that captures the rhythm and speed of his typing.

In order to "enroll" in a system, an individual presents his "live" biometric a number of times so the system can build a composition or profile of his characteristic, allowing for slight variations (different degrees of pressure when he places his finger on the reader). Depending upon the purpose of the system, enrollment could also involve the collection of other personally identifiable information.

Extraction

Commercially available biometric devices generally do not record full images of biometrics the way law enforcement agencies collect actual fingerprints. Instead, specific features of the biometric are "extracted." Only certain attributes are collected (particular measurements of a fingerprint or pressure points of a signature). Which parts are used depends upon the type of biometric, as well as the design of the proprietary system.

This extracted information, sometimes called "raw data," is converted into a mathematical code. Again, exactly how this is done varies among the different proprietary systems. This code is then stored as a "sample" or "template." The specific configuration of a system will dictate what, how, and where that information is stored. Regardless of the variations, all biometric systems must create and retain a template of the biometric in order to recognize or verify the individual. While the raw data can be translated into a set of numbers for the template, commercial biometric systems are generally designed so that the code cannot be re-engineered or translated back into the extracted data or biometric.

Comparison and Matching

To use a biometric system, the specific features of a person's biometric characteristic are measured and captured each time he presents his "live" biometric. This extracted information is translated into a mathematical code using the same method that created the template. The new code created from the live scan is compared against a central database of templates in the case of a one-to-many match, or to a single stored template in the case of a one-to-one match. If it falls within a certain statistical range of values, the match is considered to be valid by the system.

HOMELAND SECURITY SYSTEMS

Since 2000, terms such as “homeland security” and “homeland defense” have been widely used to describe America’s response to the information warfare (IW) waged by terrorists (IW will be discussed in greater detail in Chapters 13 through 19). Let’s look further into this last computer forensics system: homeland security.

Homeland Security Defined

The terms *homeland security* and *homeland defense* have received increased attention since the tragic events of September 11, 2001. While these terms are relatively new, the concepts behind them are not. Homeland security is defined as the deterrence, prevention, and preemption of and defense against aggression targeted at U.S. territory, sovereignty, population, and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies. Homeland defense on the other hand is a subset of homeland security. It is defined as the deterrence, prevention, and preemption of and defense against direct attacks aimed at U.S. territory, population, and infrastructure. In other words, you might consider homeland security to encompass policies, actions, and structures designed to protect the rights and freedoms inherent in the U.S. Constitution and homeland defense a subset of homeland security with policies, activities, and actions designed to defend against extra-territorial threats, including preemptive operations. Nevertheless, the homeland security space is still being defined. A homeland security industry is still emerging.

Homeland Security Today

In November 2002, President Bush signed the Homeland Security Act of 2002, creating the Department of Homeland Security. The new department absorbs responsibilities from 22 agencies including the U.S. Coast Guard, Border Patrol, and Secret Service.

This is the most significant transformation of the U.S. government in over a half century. The creation of this cabinet-level agency is an important step in the president’s national strategy for homeland security. The Department of Homeland Security has the following organizational structure:

- Border and transportation security
- Emergency preparedness and response
- Chemical, biological, radiological, and nuclear countermeasures
- Information analysis and infrastructure protection

Emergency mangers had been pleased with Bush's previous attention to emergency management. He was the first president to give the FEMA director an office in the West Wing. Now, emergency managers are concerned, as FEMA has been swallowed up in a new organization with a broader mission. Time will tell, but those who respond to and manage emergencies have much to do with the response to terrorist events.

The first line of homeland defense in any emergency is the "first responders"—local police, firefighters, and emergency medical professionals. Local first responders are the ones who will save lives and deal with the consequences of a terrorist attack. Emergency management and health care capabilities are a critical second tier to the first responders. While the U.S. is well prepared for "normal" emergencies, it does not currently possess adequate resources to respond to the full range of terrorist threats that are faced. Homeland security initiatives will likely focus on improving our capability to respond to a terrorist attack.

Emergency Managers and Homeland Security

Homeland security includes management of the consequences of terrorist acts and aggression and other domestic emergencies. This is the part of homeland security where first responders and emergency mangers play a vital role.

Emergency management is defined as a process to reduce loss of life and property and to protect assets from all types of hazards through a comprehensive, risk-based, emergency management program of mitigation, preparedness, response, and recovery. Emergency managers have been providing homeland security and homeland defense services for decades. During the Cold War this was called "civil defense" and the chief threat was a nuclear attack. Today, comprehensive emergency management, homeland security, and terrorism preparedness are included in an all-hazards comprehensive emergency management program (CEMP). Most emergency managers believe that homeland security should be included in a CEMP rather than developed as a separate program.

How Comprehensive Emergency Management Addresses Homeland Security

Finally, a CEMP is an overarching process that includes mitigation, preparedness, response, and recovery. A good program will address homeland security issues as well as continuity of operations, continuity of government, and related areas. Sound emergency management practices are required to mitigate the impact of day-to-day disruptions as well as managing response to and recovery from terrorist attacks and other disasters.

SUMMARY

During the past four years, management of enterprise businesses (and governments) has increased its expectations of IT security's ability to provide advance warning of electronic threats to organizations' business operations and IT infrastructure. These expectations are being made against a backdrop of external threats that have grown in both number and sophistication, internal threats that could involve terrorist and organized crime, and a rapid growth in the number and type of threat data sources.

The requirements for IT security increasingly demand integration between areas of physical security such as video surveillance and building access systems to provide a correlation with IT security's traditional tools of trade such as access logs and intrusion detection systems. The latter also creates challenges within an organization's personnel structure since an integrated security system now requires IT and non-IT data inputs that extend far beyond the traditional scope of IT.

The integration and correlation of physical security inputs with traditional IT security inputs creates requirements to improve the usefulness derived from analysis of these significantly larger volumes of unstructured data. At the same time, most enterprises are facing a difficult economic environment with infrastructure capital and operating costs allowing minimal (if any) increases in expenditure.

The challenge faced by security personnel is to capture and analyze ever larger volumes of unstructured data and provide as close to real-time as possible information with regard to the escalation of prioritized and ranked threats that are relevant to the organization. Just as enterprise resource planning (ERP) systems provide enterprise management with financial reporting metrics that are increasingly "real-time," there is a demand that security systems quickly deliver relevant information to enable a speedy reaction to a broad range of threats.

Perhaps for most organizations, up until 2001, IT security was focused on securing the "perimeter," typically via use of a firewall and perhaps with concern focused on machines that operated within the organization's Internet de-militarized zone (DMZ). It typically involved a small number of devices and log files. However, in 2001, the Code Red and Nimda worms forcefully highlighted the deficiencies of perimeter security and the need for "security in depth." In parallel, the September 11 terrorist attack on New York's World Trade Center led to growing demands for improved correlation between widely disparate data sources. The U.S. government's national strategy for homeland security which was developed in 2002, has outlined the intelligence and early warning expectations of just such a system. Implementation of sophisticated capture and computer forensics analysis systems is already underway to meet the goals of the homeland security strategy.

Faced with increasing expectations from enterprise management and the growing sophistication of threats, the requirements upon security tools have risen dramatically during the past four years. The traditional distinctions between incident response and forensic tools are blurring because of the growing expectations put upon security tools. Hence, computer forensic systems like

- Internet security systems
- Intrusion detection systems
- Firewall security systems
- Storage area networks security systems
- Network disaster recovery systems
- PKI security systems
- Wireless network security systems
- Satellite encryption security systems
- IM security systems
- Net privacy systems
- Identity management security systems
- Identity theft prevention systems
- Biometric security systems
- Homeland security systems

are now expected to deliver near real-time analysis of threats with a view to prevention and not just recovery. Thus, this chapter analyzed how computer forensics technologies can be extended to address the future requirements of IT security and computer forensics systems.

Now let's look at some of the more common conclusions that computer forensics systems can hope to answer. The following conclusions are not exhaustive, nor is the order significant.

Conclusions

- Internet security systems can provide a more secure solution, as well as one that is faster and less expensive than traditional solutions compared to security problems to employees photocopying proprietary information, faxing or mailing purchase orders, or placing orders by phone.
- Intrusion detection systems help computer systems prepare for and deal with attacks.
- Firewall security system gateways provide choke points at which security and auditing can be imposed.

- Storage area network security systems offer the most promising solutions for secure storage problems today, complementing the other solutions of direct storage, centralized storage, and network-attached storage.
- NDR systems have the ability to respond to an interruption in network services by implementing a disaster recovery plan to restore an organization's critical business functions.
- PKI security systems assume the use of *public key cryptography*, which is the most common method on the Internet for authentication of a message sender or encryption of a message.
- Companies are still ill-prepared to head off wireless network security breaches and debilitating viruses.
- Governments and organizations around the world can use satellite encryption security systems to help preserve vital national secrets, limit attacks on a nation's information infrastructure, and eliminate security and authentication obstacles to electronic commerce.
- IM management and security systems act as proxies for IM traffic going into the network, which imposes policies before letting traffic through.
- All types of organizations need to develop net privacy policies that maximize the benefit of reusing information in as many ways as possible while minimizing the risks associated with potential privacy violations.
- Identity management security systems are really about being able to manage the full life cycle of a digital identity from creation and maintenance to termination, as well as enforce organizational policies regarding access to electronic resources.
- In today's environment, it is next to impossible to stop a determined identity thief.
- Regardless of the variations, all biometric security systems must create and retain a template of the biometric in order to recognize or verify the individual.
- Homeland security systems encompass policies, actions, and structures designed to protect the rights and freedoms inherent in the U.S. Constitution. Homeland defense is a subset of homeland security with policies, activities, and actions designed to defend against extra-territorial threats, including preemptive operations.

An Agenda for Action

When completing the Forensics Systems Types Checklist (Table F3.1 in Appendix F), the computer forensics specialist should adhere to the provisional list of actions for some of the principle types of computer forensics systems. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions/exercises, hands-on projects, case projects, and optional team case project. The answers and/or solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Internet security can provide a more secure solution, as well as one that is faster and less expensive than traditional solutions to security problems of employees photocopying proprietary information, faxing or mailing purchase orders, or placing orders by phone.
2. True or False? Intrusion detection systems prevent computer systems from preparing for and dealing with attacks.
3. True or False? The firewall you decide to use will not prevent most of the attacks on your network; however, firewalls will protect against dial-in modem attacks, virus attacks, or attacks from within your company.
4. True or False? SANs are a relatively new methodology for attaching storage—whereby a separate network (separate from the traditional LAN) connects all storage and servers.
5. True or False? NDR is the ability to respond to an interruption in network services by implementing a disaster recovery plan to restore an organization's critical business functions.

Multiple Choice

1. Establishing a corporate Internet security policy involves the following, except:
   A. High-level management policy statement
   B. Systematic analysis of organization's assets
   C. Examination of risks
   D. Low-level management policy statement
   E. Developing an implementation strategy
2. Some of the many applications of smart cards include the following, except:
   A. Stored value card: minimizes the need to carry cash, can be used to purchase items from merchants, vending machines, and pay phones

B. Health care: portable, customized health care file with medical emergency data and HMO and insurance information

C. Access control in offices and hotels: allows storage of time entered and exited, access conditions, and identity

D. Contactless tickets for ski resorts and airlines: increases speed, convenience, and security and facilitates baggage checking

E. Contact tickets for ski resorts and airlines: increases speed, convenience, and security and facilitates baggage checking

3. Intrusion detection systems perform a variety of functions, except:

   A. Monitoring and analysis of user and system activity

   B. Deleting tightly bound services

   C. Auditing of system configurations and vulnerabilities

   D. Assessing the integrity of critical system and data files

   E. Recognition of activity patterns reflecting known attacks

4. Firewalls act as a barrier between corporate (internal) networks and the outside world (Internet) and filter incoming traffic according to a security policy. This is a valuable function and would be sufficient protection were it not for the following facts, except two:

   A. Improved firewall flexibility and upgradability.

   B. Not all access to the Internet occurs through the firewall.

   C. Not all threats originate outside the firewall.

   D. Firewalls themselves are subject to attack.

   E. Unflexibility and gradability that firewalls do not provide.

5. In today's world, corporations face a variety of information system attacks against their LANs and WANs. Many of these attacks are directed through the Internet. These attacks come from three basic groups, except two:

   A. Persons who see attacking a corporation's information system as a technological challenge

   B. Persons with no identified political or social agenda who see attacking a corporation's information system as an opportunity for high-tech vandalism

   C. Persons who investigate to avoid the possibility of incurring legal action against themselves or the organization for whom they are reviewing the investigation

   D. Persons who need to investigate to avoid the possibility of incurring legal action against themselves or the organization for whom they are conducting the investigation

   E. Persons associated with a corporate competitor or political adversary who see the corporation's information system as a legitimate strategic target

Exercise

Larry deposits a stolen third-party check into his account. No problems are detected during check clearance, and two days later cleared funds are available in Larry's account. Subsequently an ATM camera records Larry making a cash withdrawal. The bank's forensics system analyzes the video image and a match is found against the latest police records of Larry, wanted in connection with illegal drug activities. How would your forensic system continue to handle this analysis?

HANDS-ON PROJECTS

At 9:36 A.M. William swipes his access card to level 20 and enters the secure staff area. Two hours pass and the forensics system detects that Bill has yet not logged into his computer. The system checks the company calendar and detects that Bill, a member of the organization's merger and acquisition unit, is scheduled for an off-site training course and is not expected in the building at all that day. The system reviews the video log files of level 20 for that day and cannot find any match for Bill against the staff photo database; however, it has detected an unknown person entering the floor at 9:36 A.M. The system rechecks the company calendar for other staff members attending the same off-site training course and determines that one other person, Jennifer, a team leader within the organization's HR department was logged by the building access system as entering the secure area on level 36 at 10:48 A.M. The system reviews the level 36 video log files and detects that the same unidentified person has used Jennifer's access card to enter the level 36 secure area. The system review of related video log files confirms the same unidentified person leaving level 20 at 9:54 A.M. and leaving level 36 at 10:50 A.M. At this point, how would the company's computer forensics team go about investigating this case?

Case Project

Karin enters a bank branch in the Chicago area and deposits a check for her brother. The bank video camera captures an image of Karin entering the branch and matches it against its database of customers. The image is time and date stamped. Later that day, Karin's savings account is accessed via Internet banking from an IP address located in Turin, Italy. During a routine correlation of data, the apparent discrepancy is detected by the bank's forensics system. How would you as a computer forensics specialist, go about investigating this incident?

Optional Team Case Project

When a senior executive of a multimillion-dollar international organization suddenly resigned during an internal audit, the computer forensic technology team was called in to find out why. Please explain your solution in detail regarding the organization's computer forensic technology team's investigation into this matter.

REFERENCES

[1] Duncan, Mark, "Internet Security," 610 Gilbert Avenue, Suite 19, Menlo Park, CA 94025, 2002.

[2] "Online Payment Processing: What You Need to Know," © 2003 VeriSign, Inc. All rights reserved. VeriSign Worldwide Headquarters, 487 East Middlefield Road, Mountain View, CA 94043, 2003.

[3] Bace, Rebecca, "An Introduction to Intrusion Detection Assessment," ICSA Labs, Cybertrust, Corporation Headquarters, 13650 Dulles Technology Drive, Suite 500, Herndon, VA 20171, 2004.

This page intentionally left blank

4 Vendor and Computer Forensics Services

Cyber crime costs U.S. businesses millions, if not billions, of dollars in unrealized profits and exposes organizations to significant risk. And it is on the rise. In 2003, the Computer Emergency Response Team (CERT) reported a sevenfold increase in the number of computer security incidents reported in 2002.

As information technology and the Internet become more integrated into today's workplaces, organizations must consider the misuse of technology as a real threat and plan for its eventuality. When cyber crime strikes, the issue is not the incident itself, but how the organization responds to the attack.

This chapter looks at how a swift and measured forensic incident response, drawing on sound policies, vendor tools, and support, allows an organization to contain the potential damage of an attack and effectively seek compensation or prosecution. In addition, this chapter covers the following computer forensic services:

- Forensic incident response
- Evidence collection
- Forensic analysis
- Expert witness
- Forensic litigation and insurance claims support
- Training
- Forensic process improvement

OCCURRENCE OF CYBER CRIME

Cyber crime occurs when information technology is used to commit or conceal an offense. Computer crimes include:

- Financial fraud
- Sabotage of data or networks
- Theft of proprietary information
- System penetration from the outside and denial of service
- Unauthorized access by insiders and employee misuse of Internet access privileges
- Viruses, which are the leading cause of unauthorized users gaining access to systems and networks through the Internet [1]

Cyber crimes can be categorized as either internal or external events. Typically, the largest threat to organizations has been employees and insiders, which is why computer crime is often referred to as an insider crime. For example, Ernst & Young's global research has found that 93% of all identified frauds were committed by employees, almost 44% of which were committed by management.

Internal events are committed by those with a substantial link to the intended victim, for example, a bank employee who siphons electronic funds from a customer's account. Other examples include downloading or distributing offensive material, theft of intellectual property, internal system intrusions, fraud, and intentional or unintentional deletion or damage of data or systems.

However, as advances continue to be made in remote networks, the threat from external sources is on the rise. For example, in the 2003 CSI/FBI Computer Crime and Security Survey, 50% of respondents reported their internal systems as a frequent point of attack, while 59% reported Internet connections as the most frequent point of attack [2].

An external event is committed anonymously. A classic example was the Philippine-based 1999 "I Love You" email attack. Other types of external cyber crime include computer system intrusion, fraud, and reckless or indiscriminate deliberate system crashes.

Internal events can generally be contained within the attacked organization, as it is easier to determine a motive and therefore simpler to identify the offender. However, when the person involved has used intimate knowledge of the information technology infrastructure, obtaining digital evidence of the offense can be difficult.

An external event is hard to predict, yet can often be traced using evidence provided by, or available to, the organization under attack. Typically, the offender has no motive and is not even connected with the organization, making it fairly straightforward to prove unlawful access to data or systems.

CYBER DETECTIVES

Computer forensics, therefore, is a leading defense in the corporate world's armory against cyber crime. Forensic investigators detect the extent of a security breach, recover lost data, determine how an intruder got past security mechanisms, and, possibly, identify the culprit. Forensic experts need to be qualified in both investigative and technical fields and trained in countering cyber crime. They should also be knowledgeable in the law, particularly legal jurisdictions, court requirements, and the laws on admissible evidence and production.

In many cases, forensic investigations lead to calling in law enforcement agencies and building a case for potential prosecution, which could lead to a criminal trial. The alternative is pursuing civil remedies, for instance, pursuing breach of trust and loss of intellectual property rights.

Legal Issues

The most common legal difficulty faced by organizations seeking to redress cyber crime in the courts is having digitally based evidence accepted. Notwithstanding the technical expertise of information technology (IT) teams, most companies are ill-equipped to investigate cyber crime in a way that results in the collection of admissible evidence. For example, data collected as evidence must be shown to not be tampered with and be accounted for at every stage of its life from collection to presentation in court. In other words, it must meet the requirements of the jurisdiction's laws of evidence.

Another issue is the lag time between legislation and change and improvements in technology. As a result, law enforcement organizations and computer forensic experts are often forced to use archaic and nonspecific laws to fit unusual circumstances.

For example, to commit *theft*, a person must permanently deprive the victim of property. However, if a disgruntled employee copied an organization's database and sold it to a rival company, the organization is not permanently deprived of the data; therefore, technically, no offense of *theft* has been committed. In addition, it is unclear whether *data* fits into the legal definition of property. However, even in cases where there is a clearly defined crime, corporations are often hesitant to pursue a criminal conviction because of the time, cost, and reputation risk involved in reaching a legal outcome.

FIGHTING CYBER CRIME WITH RISK-MANAGEMENT TECHNIQUES

The rate of technological change, the spread of computer literacy, and the growth of e-commerce [3] collaboration, such as alliances and marketplaces, make the challenge of restricting cyber crime damage daunting. With legislation lagging behind technology, businesses have had no choice but to absorb the responsibility for the security of their most valuable asset—their information. Risks range from expensive downtime, sales and productivity losses to corrupted data, damage to reputation and consumer confidence and loyalty, and hefty compensation payments or lawsuits for breaches of client information.

The best approach for organizations wanting to counter cyber crime is to apply risk-management techniques. The basic steps for minimizing cyber crime damage are creating well-communicated IT and staff policies, applying effective detection tools, ensuring procedures are in place to deal with incidents, and having a forensic response capability.

Effective IT and Staff Policies

Well-communicated and "plain English" IT policies educate staff about their rights and obligations in the workplace. The goal of these policies is to create a security solution that is owned by all staff, not only by those in the IT division. To be effective, IT policies should make plain what an individual employee can and cannot do on the organization's systems and the legal implications of misuse. It is also vital to make a continuing investment in policies, which must evolve and be supported by ongoing training initiatives.

Effective policies diminish the risk of internal attack, particularly unintentional attack. In addition, when attack does occur, these policies clearly define what constitutes a breach of security, making it easier to prosecute or seek compensation from the perpetrator.

Vendor Tools of the Trade

Although internal policies will not dissuade external cyber criminals, the right vendor tools will detect an external attack and alert the organization to the threat. These tools are programs that either analyze a computer system to detect anomalies, which may form the basis of an attack, or locate data that can be used as evidence of a crime or network intrusion.

Choosing the right cyber crime detection tools is essential for risk management in all organizations, but like most applications associated with an organization, the question is, what is the right tool? The right tools are those that deliver appropriate information that the forensic expert can interpret to achieve the best outcome. Ultimately, the evidence must withstand the rigors of legal proceedings. To deliver the information needed, software tools should be probing (without compromising the target of interrogation), concise, able to report findings fully, supported, and easy to use. Such tools will save forensic experts valuable time and allow them to concentrate on data interpretation.

The 2003 CSI/FBI Computer Crime and Security Survey shows a significant increase in companies using intrusion detection systems, from 58% in 2001 to 79% in 2003 [2]. Although some attacks will not be prevented, damage such as financial loss or negative publicity can be contained with early warning.

As with all of today's technology, detection tools date quickly as new threats emerge. Effective detection tools need to constantly evolve to counter these threats and must be engineered around best-practice risk management associated with vulnerabilities, system configurations, and viruses. Some online products and services currently on the market provide efficient, cost-effective solutions by accessing computer vulnerabilities specific to an organization's IT environment.

Effective Procedures

Even in an organization that has implemented the hardware, installed the software, produced the policies, and employed competent staff to run an effective IT environment, it is not possible to prevent an incident from occurring. However, the attack itself does not have the greatest impact on a company. How the business responds to that attack has the greatest impact on a company. Without the appropriate procedures in place to counter detected attacks, an organization is exposed to the risks of lost data, financial loss, network damage, and loss of reputation.

Although many different types of attacks may occur, the majority require the same basic steps of response. For example, the simple process of ensuring that the right people know about the incident when it happens enhances an organization's response, both in time and effective handling procedures.

Forensic Response Capability

When an incident occurs, an organization needs an appropriate forensic response in place. By appointing a forensic expert to manage the response to an incident, organizations ensure all avenues are canvassed, all evidence located and handled correctly, and all those involved treated impartially (see sidebar, "Computer Forensic Incident Response Procedures [CFIRP]").

COMPUTER FORENSIC INCIDENT RESPONSE PROCEDURES (CFIRP)

Let's look at an incident that occurred at a well-known technical university that clearly shows the need to have an enforceable and workable CFIRP:

Picture this: it is 1 A.M. and email comes into the security mailing list from an outside source informing you that this site's server has been compromised, and from the logs two of the machines in your domain look to also have been compromised. The only people on the mailing list who are up and awake and reading their mail are the operations staff, but they know that sometimes in the wee hours, one of the more nocturnal network staff come in. They take a chance and call his office. To their delight, he is in his office, so they forward him the security email and consider their part of this incident finished.

The nocturnal network person reads the email, looks at the time, and decides to block those two hosts at the router from the Internet. He then sends an email to security stating that the hosts are blocked and considers his part in this incident finished.

The next morning the rest of the security team trickles in and reads the security mail along with about 500 other emails of various severities. The entire team assumes that the nocturnal network person notified the owner of the machines of the problem and that action has been taken. You all get on with other business, and of course the nocturnal network person, being nocturnal, is not around to correct your assumptions.

OUTCOME

The two servers that were blocked were two major servers for the math department. They both had high-profile off-site collaborative projects going on . The math department has their own system administrators, who were not on the security mailing list.

The system administrators spent all of that day and part of the next troubleshooting their server and network, trying to figure out why they could not get to the Internet. No one informed the owners of the alleged compromised hosts of the network block of the alleged compromise until the problem was elevated to the director of networking and the chair of the math department.

Where to start is the first question that comes to mind. You should start with an outline of the key elements of a successful CFIRP but also include forms that can be used to identify the incident contact personnel as well as forms for incident handling, containment, and eradication.

Not having an incident response policy in place can lead to serious liabilities for your company or university, as well as for the system administrator who is working

→

on the incident. There may be times when local law enforcement will pay you a visit. It is a very good idea to know what information can be given out without a search warrant, and in the case of a warrant, who in your organization should receive the warrant. Knowing someone in your local computer crimes lab is a good idea. Having good communications with them before you are responding to a critical incident will make life much easier.

The FBI has developed a collaborative effort, named InfraGard. This description of the organization is taken from their Web page: "*InfraGard* is a cooperative undertaking between the Federal Bureau of Investigation and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants, that is dedicated to increasing the security of the critical infrastructures of the United States of America" [3a].

It is also critical to have someone assigned to notify and report incidences to CERT. This can be called out clearly in your CFIRP so everyone knows what they are responsible for and you can cut down on redundant reporting.

Last but certainly not least, let's not forget that an ounce of prevention is worth a pound of cure. Educating your user community will help decrease the number of security incidents you have. It's been proven time and time again that most security problems originate from inside organizations.

Having a clear and concise conditions of use policy as well as a policy for departmental computers on your network will prove invaluable in resolving internal security violations. When developing your policy, a lot will depend on the type of organization. Government policies differ from private sector policies [4], and university policies are in their own category, being even more specific, depending on whether they are public or private institutions.

If you don't think you need a CFIRP policy, try the following exercise: Do a mock incident (with the permission of your management), but don't let your security people know it is an exercise.

The difficult part of creating a CFIRP is that it has to be tailored for your site. You will need to take into consideration all the nuances of your site and get support and buy-in from upper management. Best of luck to you; it will be well worth the work [5].

In other words, deterrence is the appropriate forensic response and the fundamental element of a defensive strategy for the organization. However, for deterrence to be effective, potential antagonists must be convinced that they will be identified and punished swiftly and severely. This is the essence of the three key causal variables of general deterrence theory: certainty, severity, and celerity. Unfortunately, while the methods for identifying perpetrators of crimes in the law enforcement context, and attackers in the military context, are well developed, similar capabilities do not currently exist for the networked cyber realm. Thus, while deterrence is recognized as a highly effective defensive strategy, its applicability to defense against attacks on our nation's information infrastructures is not clear, mainly because of our inability to link attackers with attacks.

A conceptual tool that can help visualize and understand the problem is to think of a thread, or sequence, of steps (with requisite technologies) necessary to effect a deterrent capability. As with the "weak link" and "picket fence" analogies, if any one of these steps is missing or ineffective, the ability to achieve the desired result is compromised.

Looking at this thread, you can see that current intrusion detection technology is focused primarily on the first element in the sequence above. Any response is generally limited to logging, reporting, and isolating or reconfiguring. What is missing is the ability to accurately identify and locate attackers and to develop the evidentiary support for military, legal, or other responses selected by decision makers. While defensive techniques are important, it's critical not to "stovepipe" in such a way that you can't effectively link with the offensive component of an overall strategic cyber defense.

In addition to detecting the attacks, perhaps you should also develop a "forensic," or identification, capability to pass the necessary "targeting" information on to the offensive components of the response team, regardless of whether the response is through physical or cyber means. Such a capability is critical if your cyber defenses are to transcend a merely reactive posture to one in which both offensive and defensive techniques can be effectively applied in tandem. This is in line with the established principles of war, which suggest that an offensive (and therefore deterrent) spirit must be inherent in the conduct of all defensive operations. Forensics response capabilities could help provide the bridge between the defensive and offensive elements of an overall cyber defense strategy. Accurate and timely forensic response techniques would also enable the effective use of the three elements of deterrence. Otherwise, attackers can act with impunity, feeling confident that they need not fear the consequences of their actions.

Forensics is a promising area of research that could help provide the identification and evidence necessary to support an offensive response against attacks on your information infrastructure, regardless of whether that response is executed through physical, information warfare (IW), or other means. Although forensic response techniques are highly developed for investigations in the physical realm and are being developed for application to computer crime, what is needed is an analogous capability for real-time, distributed, network-based forensic response analysis in the cyber realm. It would seem appropriate to incorporate the collection of forensic response data with the intrusion detection and response types of technologies currently being developed. Critical supporting technologies include those needed for correlation and fusion of evidence data, as well as automated damage assessment.

The importance of solid identification and evidence linking an attacker with an attack will be critical in the increasing complexity of the networked information environment. Cyber attacks against the U.S. and its allies may not have the obvious visual cues and physical impact typically associated with attacks in the physical realm. In these cases, the available courses of action will be heavily influenced by various political, legal, economic, and other factors. Depending on the situation, it may be necessary to have irrefutable proof of the source of the attack, the kind of proof typically developed through forensic response methods.

For example, one suggested concept is for a "cyberspace hot pursuit" capability to aid in the back-tracing of incidents to discover perpetrators. Use of such a capability implies the need for laws specifying authorization to conduct cyberspace pursuits and cooperative agreements with foreign governments and organizations. A second suggestion is for the development of a tamper-proof, aircraft-like "black box" recording device to ensure that when an incident occurs and is not detected in real time, the trail back to the perpetrator does not become lost.

Extending the aircraft analogy, the need for effective identification during cyberspace pursuits, and for coordinating offensive IW response actions through intermediary "friendly" networks, may necessitate a type of "network identification friend or foe (IFF)" capability, just as the introduction of fast-moving aircraft in the physical realm necessitated the need for secure IFF. Although the need for IFF has traditionally been a concern at the tactical level of warfare, the failure to effectively deal with such issues could certainly have strategic implications.

One issue of concern at the strategic level of IW is the distinction between the military and private sector information infrastructures. It is clearly not feasible to require the private sector to secure its systems to the level required for military networks. The approach suggested in this section may be applicable regardless of whether the networks attacked belong to the military. For example, in the physical realm today, if a civilian target is struck, the FBI and other federal agencies are called in to assist and investigate the incident, and when the identity of the attackers is determined, appropriate legal, political, or military actions are taken in response. From an organizational perspective, efforts are underway to develop the necessary coordination structures, such as the National Infrastructure Protection Center, between the private and commercial sectors. From a technical perspective, major elements of the commercial infrastructure could participate in a national-level monitoring system, while private entities could maintain their own in-house capabilities with the ability to provide necessary data to national authorities following an incident just as would be the case with the FBI being called in to investigate a crime.

Another fundamental concern this approach may help address is the problem of malicious insiders. The security paradigm of enclaves separated by boundary controllers is most effective against attacks from the outside. Attacks initiated from within the enclave, possibly even by a trusted insider, have traditionally been much harder to defend against. Cyber forensics response techniques may provide the capability needed to deal with this problem, which simply cannot be addressed by traditional security techniques based on privileges. These systems simply check whether a user is acting within the prescribed privileges while remaining in complete oblivion regarding the abuse of these privileges.

In other words, as previously discussed, a deterrence-based approach is an element of an overall cyber defense strategy. The need for timely and unequivocal identification of attackers is essential for such an approach to be effective. Unfortunately, the technical basis for such identification has not received much attention from the research and development community. In addition, there may be some complicating factors for the implementation of the type of identification and forensics response capability discussed here, such as the widespread move to encryption. However, until research and development resources are committed to investigation of the relevant issues, the extent of the challenge cannot be fully understood.

COMPUTER FORENSICS INVESTIGATIVE SERVICES

There are without doubt some very knowledgeable experts in the field of computer forensics investigations; however, there has been an increase in the number of people purporting to be experts or specialists who produce flawed opinions or take actions that are just plain wrong. The reasons for these errors are manifold but range from peer or management pressure, restricted timescales, and problems with software, to sheer lack of knowledge. Most investigations are basically the same in that they are either proving or disproving whether certain actions have taken place. The emphasis depends on whether the work is for the accuser or the accused.

In many companies, forensic computer examiners are *kings* because they have more knowledge of the subject than their peers. However, they are still subject to management pressures to produce results, and at times this can color their judgment. Time restrictions can cause them to take short cuts that invalidate the very evidence they are trying to gather, and when they do not find the evidence that people are demanding (even if it isn't there), they are subject to criticism and undue pressure.

Many of these *specialists* are well meaning, but they tend to work in isolation or as part of a hierarchical structure where they are the *computer expert*. The specialists' management does not understand what they are doing (and probably don't want to admit it), and often they are faced with the question, Can't you just say this.....? It takes a very strong-minded person to resist this sort of pressure, and it is obvious that this has had an adverse effect in a number of cases.

This sort of pressure comes not only from within the organizations, but also from external sources. When you reply with: "I'm sorry it's just not there" or "No, the facts do not demonstrate that," you frequently end up with lengthy high-pressure discussions with the client, which appear to be designed to make you doubt your own valid conclusions.

Working in isolation is a major problem; apart from talking to yourself (first sign of madness), many people have no one else to review their ideas and opinions. This is where having recourse to a team of investigators, software engineers, hardware engineers, and managers who understand (not always a good thing, depending on your point of view) any doubts or unusual facts, is valuable for fully discussing and investigating to ensure that the correct answer is found.

Computer Intrusion Detection Services

Installing technical safeguards to spot network intruders or detect denial-of-service attacks at e-commerce servers is prudent, but if your staff doesn't have the time or skills to install and monitor intrusion detection software, you might consider outsourcing the job.

Intrusion detection is the latest security service to be offered on an outsourced basis, usually by the types of Internet service providers (ISPs) or specialized security firms that have been eager to manage your firewall and authentication. Although outsourcing security means divulging sensitive information about your network and corporate business practices, some companies say they have little choice but to get outside help, given the difficulty of hiring security experts [6].

For example, the Yankee Group reports that managed-security services (of which intrusion detection is the latest phenomenon) more than tripled, from $450 million in 2000 to $1.5 billion in 2003. By 2009, the market is expected to reach $7.4 billion, fueled by the trend toward outsourcing internal local area network (LAN) security to professional security firms as *virtual employees*.

Digital Evidence Collection

Perhaps one of the most crucial points of your case lies hidden in a computer. The digital evidence collection process not only allows you to locate that key evidence, but also maintains the integrity and reliability of that evidence. Timing during this digital evidence collection process is of the essence. Any delay or continued use of the suspect computer may overwrite data prior to the forensic analysis and result in destruction of critical evidence (see sidebar, "Evidence Capture"). The following are some helpful tips that you can follow to help preserve the data for future computer forensic examination:

- Do not turn on or attempt to examine the suspect computer. This could result in destruction of evidence.
- Identify all devices that may contain evidence:
  - Workstation computers

  - Off-site computers (laptops, notebooks, home computers, senders and recipients of email, PDAs, etc.)
  - Removable storage devices (zips, Jaz, Orb, floppy diskettes, CDs, Sony Memory Sticks, Smart Media, Compact Flash, LS-120, optical disks, SyQuest, Bernouli, microdrives, pocketdrives, USB disks, firewire disks, PCMICA)
  - Network storage devices (redundant array of independent [or inexpensive] disks [RAIDs], servers, storage area networks [SANs], network attached storage [NAS], spanned, remote network hard drives, back-up tapes, etc.)
- Quarantine all in-house computers:
  - Do not permit anyone to use the computers.
  - Secure all removable media.
  - Turn off the computers.
  - Disconnect the computers from the network.
- Consider the need for court orders to preserve and secure the digital evidence on third party computers and storage media.

EVIDENCE CAPTURE

One of the fundamental principles of computer investigation is the need to follow established and tested procedures meticulously and methodically throughout the investigation. At no point of the investigation is this more critical than at the stage of initial evidence capture. Reproducibility of evidence is the key. Without the firm base of solid procedures that have been strictly applied, any subsequent antirepudiation attempts in court will be suspect and the case as a whole likely to be weakened.

Another frequent problem with capturing evidence is lack of experience—not only lack of site experience but also inappropriate experience of the type of systems that might be encountered. One of the most difficult skills on-site is knowing when to call for help. It is essential that a sympathetic working environment is created such that peer pressure or fear of loss of status and respect does not override the need to call for help. Easier said than done perhaps, but no less essential for that reason.

Finally, sloppiness, time pressure, pressure applied on-site, fatigue, or carelessness have all been contributory factors in transforming solid computer evidence into a dubious collection of files. These avoidable issues come down to individual mental discipline, management control and policy, and selecting appropriate staff to carry out the work. They are issues for which there is no sympathy. This is bad work, plain and simple.

Ultimately, any time the collection of computer evidence is called into question, it is potentially damaging to everyone who is a computer forensic practitioner; it is ultimately in everyone's best interest to ensure that the highest standards are maintained.

Next, let's briefly look at drafting a comprehensive and effective computer forensics policy. This type of computer forensics service is used by countless organizations (banks, insurance companies, law firms, local governments, retailers, technology firms, educational institutions, charitable organizations, manufacturers, distributors, etc.).

Computer Policy

Often overlooked, detailed policies on the use of computers within an organization are an ever-increasing necessity. Corporations and government agencies are racing to provide Internet access to their employees. With this access, a Pandora's box of problems is opened. Paramount is loss of productivity; workers can easily spend countless hours online entertaining and amusing themselves at their employer's expense. A hostile workplace environment can be created through pornography, potentially exposing the organization to civil liability.

Although protecting your organization from outside threats is clearly important, protecting the organization from internal threats is at least as important, if not more so. According to the 2003 Computer Crime and Security Survey conducted by the Computer Security Institute and the FBI, 67% of the respondents reported unauthorized access to information by persons inside the organization, compared to just 42% who reported intrusions by outsiders. A quarter reported theft of proprietary information, and 80% reported theft of laptop computers. Virus contamination was reported by 92%, and a staggering 99% reported systems abuse by insiders (pornography, pirated software, inappropriate email usage, etc.). According to Sextracker, an organization that tracks the online pornography trade, 82% of online pornography viewing occurs during the 9–5 work day [2].

Your computer forensics policy manual should therefore address all manners of computer-related policy needs. The content should be based on your corporation's experience in employment-related investigations, computer crime investigations, civil litigation, and criminal prosecutions. Approximately half of the manual should consist of detailed discussions of each of the policy topic areas; the other half should be sample policies that can be readily customized for your organization. The discussions should include topics such as why policies are needed, potential liability, employee productivity considerations, and civil litigation. Safeguarding critical and confidential information should be discussed in detail. The policies should directly address the problems that you would typically find in organizations of all sizes.

Now let's look at another computer forensics service: litigation support and insurance claims. As the risk increases, so will the interest in policies and the cost of premiums and litigation.

Litigation Support and Insurance Claims

Since its inception, cyberinsurance has been billed as a way for companies to underwrite potential hacking losses for things technology cannot protect. The concept of insuring digital assets has been slow in catching on because the risks and damages were hard to quantify and put a price tag on.

The September 11, 2001, terrorist attacks quickly elevated corporate America's interest in cyberinsurance, as industry magnates looked for ways to mitigate their exposure to cyberterrorism and security breaches. At the same time, it has become harder to find underwriters willing to insure multimillion-dollar cyberspace policies. For carriers willing to sell such paper, the premiums have skyrocketed. Prior to September 11, 2001, the focus of information security was on critical infrastructure. After September 11, 2001, the focus has shifted to homeland defense and trying to understand whether financial institutions and other critical infrastructure such as telecommunications are vulnerable to cyberterrorism.

Insurance stalwarts such as Lloyd's of London, AIG, and Zurich now offer policies for everything from hacker intrusions to network downtime. The breadth of cyberinsurance policies is growing, from simple hacker intrusion, disaster recovery, and virus infection to protection against hacker extortion, identity theft, and misappropriation of proprietary data.

While the market was already moving to provide policies to cover these risks, many executives viewed cyberinsurance as a luxury that yielded few tangible benefits. Many risk managers buried their heads in the sand, believing they would never need anything like cyberinsurance. There was a naiveté on the part of senior management. IT managers were not willing to admit they had to fix something of that magnitude, because they were afraid to go ask for the money.

The aftermath of the 9-11-01 attacks illustrates the interconnectedness of all systems: financial services, information and communications, transportation, electrical power, fire, and police. They all relate in profound ways we are only now beginning to understand. Businesses are starting to think about what type of recovery position they would be in if something similar to the World Trade Center attack happened to them.

While the cyberinsurance market may grow in the wake of the 9-11-01 tragedy, carriers are tightening the terms and conditions of policies. Premiums are going up significantly and underwriters are hesitating to sign big policies. In the past, companies seeking a $25 million policy could find someone to cover them. Now it's much more difficult. Underwriters who didn't blink at $5 million or $10 million policies, would now rather insure $1 million policies. The marketplace is in transition, and there's undoubtedly a hardening of trading conditions for both traditional property and casualty insurance, as well as the emerging new e-commerce products.

Premiums on cyberinsurance are an easy mark for price hikes because there's little historical data on which to set them. It's difficult to pinpoint the losses if data is corrupted, a network is hacked, or system uptime is disrupted. The fear of bad publicity keeps many companies mum on hacking incidents, which makes it more difficult to collect data for projecting future losses.

To develop robust cyberinsurance, two major developments need to take place. First, sufficient actuarial data needs to be collected. Second, insurance carriers need to develop a better understanding of the IT systems in use and how they interact with other information and automated systems.

Industry analysts predict that underwriters will push any changes in cyberinsurance offerings and the systems used by policyholders. The first indication of this trend came earlier in 2001, when an underwriting company tacked a 5 to 15% surcharge on cyberinsurance premiums for users of Windows NT on Internet information services (IIS) servers, citing their poor security track record, which makes them more expensive to insure. The underwriters are going to force the issue by saying, "Look, if you lose your whole business, if things like that happen, you can expect to pay a higher premium."

FORENSIC PROCESS IMPROVEMENT

The purpose of this section is to introduce the reader to a process that will enable a system administrator or information security analyst to determine the threat against their systems and networks. If you have ever wanted to know more about who might have attacked or probed your system than just the IP address that appeared in the *var/log/messages* of your machine, then this section may help you. Although it is rare, some of these simple techniques may help you identify the perpetrator of an attack on your system. Although most system administrators are rightly concerned with first securing their hosts and networks from attack, part of doing that job correctly demands that you understand the threat against those systems and networks. The risk any system connected to the Net faces is a product of vulnerability and threat. The techniques covered in this section will help you determine possible actions and possible motivations of the attacker. If you can understand your attacker, than you can better defend against and respond to attacks against your network. Of course, it is important to understand that hackers will loop through several systems during the attack phase.

So why bother researching the apparent source of an attack? What if your system is the first system of many that the hacker will use in his or her attack against other systems? Could you be held liable for damage done by the attacker to someone else's systems? What if the attacker is operating from within a country that has no laws against hacking and can thus operate with impunity? Or what if the hacker is unskilled and has left clues behind that a skilled researcher could use to identify him or her? All of these reasons justify taking a small amount of time to research the apparent source of a serious attack or intrusion. Of course, all of these techniques should be used after you have secured your system and possibly consulted with law enforcement personnel. This should be done if the level and seriousness of the attack justify such an action. Next, let's review the tools that are used in the threat identification process.

The Tools

The tools discussed here outline a step-by-step process that will help you identify the attacking host and possible actors that may have used that host to attack your system. This section is not intended to be a tutorial for how to use each tool on its own. There are many sources of information that cover each tool by itself in more detail. Many of you are certainly familiar with or have used many of the tools discussed here at one time or another. Keep in mind that here we are talking about the overall process of characterizing the threat from a domain. The first step in the threat identification process is simply to know who owns the IP used in the attack. For detailed switchology on the use of each tool, consult the main pages or other sources for each tool listed.

It is advisable to find a Web proxy or gateway Web site for conducting any type of intelligence collection operation against the attacking host. In this way, you do not run the risk of further antagonizing or scaring off a potential intruder who might be watching the connection logs from his or her victimized host. A good all-around site that contains most of the tools discussed here is http://www.samspade.org. This site also contains a brief description of each tool and its use. For instance, to learn more about the Dig command, simply hit the More Information radio button listed beside the tool. Another useful site is http://network-tools.com.

Dig –x /nslookup

The first step in the process is to reverse the offending IP address. The Dig -x ip command will perform a reverse lookup on an IP address from its domain name server. The "-x" option will ensure that you receive all records possible about your host from the Domain Name Service (DNS) table. This might include nameservers, email servers, and the host's resolved name. The "nslookup" command, Nslookup ip, will also perform a reverse lookup of the host IP address, but will only return the resolved name.

Whois

The next step in the process is to perform a "whois" lookup on the IP address to see who owns the offending IP or at least who it is registered to. This can be a tricky operation. Use the resolved name previously mentioned to try to determine what country or region the IP address might be based in and then be sure to use the proper whois gateway for that region of the world. The main gateways are ARIN (the American Registry), APNIC (the Asian Pacific Registry), and RIPE (the European Registry). There are dozens of others, but most addresses should be registered in one of these. If your whois data does not match your resolved name, for example the resolved name *http://www.cnn.com* and the whois database ARIN indicates the registered owner is CNN network (a match), then you may have to do some more digging. Whois databases can contain outdated information. You may want to then research your IP with the country-specific whois database to determine the correct registered owner. A good collection of country-specific whois databases can be found at *http://www.allwhois.com*. For more information on conducting detailed whois queries check out *http://www.sans.org*.

Ping

Conduct the Ping ip command to determine if your attacking IP is currently online. Note that many administrators block ICMP traffic, so this is not conclusive evidence either way.

Traceroute

The next step in the process is to conduct a Traceroute ip to determine possible paths from your proxy site to the target system. Traceroute may help you in two ways. If your IP does not resolve possible paths from your proxy site to the target system, there may be a clue about its parentage. Look at the resolved host just before your target. This host's name may be the upstream provider for the attacking host and thus a point of contact or it may have the same domain as your attacking host, although that is not always true. Also, a traceroute might give you an important clue about the physical location of the attacking box. Carefully look at the path the packets traveled. Do they tell you what city they are in? Often they will. If you can determine what city the attack came from, you have just considerably narrowed down the possible pool of candidates of who the attacker might be.

Finger

Conduct a finger@ip command to determine who is currently logged onto the system that attacked you. Now, to be frank, this command will rarely work, because most administrators wisely turn this service off. However, it does not hurt to try.

Keep in mind that many systems that are compromised and used as lily pads to attack other hosts are poorly configured (that is why they were compromised in the first place). They may also have the finger service running. If it is running, finger root@ip sees the last time root was logged on and, more important, from where root was logged on. You might be surprised to see root logged on from a third system in another country. Keep following the trail as long as your commands are not refused. You should be able to trace back hackers through several countries using this simple, often-overlooked technique. Look for strange login names and for users logged into the system remotely. This may indicate where the host was compromised from and is the next clue to where to focus your research.

Anonymous Surfing

Surfing anonymously to the domain where your attacking IP is hosted is the next step in the threat identification process. You will know this domain name by looking at the resolved name of the host and the whois data. One technique that is useful is to use a search engine such as *http://www.altavista.com* with the specialized advanced search option of "+host:domain name and hack*." This query will return the Web links of possible hackers who operate from the domain name you queried. You can substitute *warez* or *mp3* and the like to focus on terms of interest specific to warez or mp3 dealers. The number of Web pages returned by the query, as well as the details on those pages, gives you an indication of the level of threat to assess to a certain domain. For example, if you were investigating a host registered to demon.co.uk (Demon Internet), you would type "+host:demon.co.uk and hack*" in the Altavista query box. You may be surprised to see a return of some 55,000-plus hacking-related pages hosted on this domain. The Demon Internet seems to harbor many hackers and, as a domain, represents a viable threat to any organization. As a standard practice, you might want to block certain domains at your firewall if you are not already blocking ALL:ALL. Another possibility to widen the search is to use "+link:domain name" in the Altavista search. This will show all Web pages that have a link to the domain in question listed on their Web page. In other words, the ever-popular "here is list of my hacker friends and their c001 hacker sites" pages will appear via this search. You will also want to keep in mind the target of the attack. What were the hackers going after? Can you tell? Conduct searches for the resources targeted and combine these terms with Boolean operators such as "and espionage." Check newswires or other competitive intelligence sources to determine, if possible, who might be going after your company's resources. A good site to use to conduct your searches anonymously is *http://www.anonymizer.com.*

USENET

The last step in the process of threat identification is to conduct a USENET traffic search on your domain. Sites such as *http://groups.google.com/* are excellent for this. Search on the attacking IP address in quotes to see if other people are reporting activity from this IP in any security newsgroups. Search on the domain name or hacker aliases that you might have collected from your anonymous surfing, or from the returns of your finger queries. You can expand the headers of the postings by clicking on "view original posting." This may show you the actual server that posted the message, even if the hacker attempted to spoof his or her mailing address in the visible header. This method can reveal the true location of your hacker. Clicking on "author profile" can also give you valuable information. Look at the newgroups your hacker posts to and look at the number and sophistication of those postings. Pay attention to off-subject postings. A hacker will often let down his guard when talking about his favorite band or hobby, for example. You can also search sites such as *http://www.icq.com* if you have a hacker alias from a defaced Web page or your Altavista search narrowed by the domain "+hacker" criteria previously noted.

Putting It All Together

Once you have completed the process previously outlined and gathered all the information from these tools, you should be able to make an educated guess about the threat level from the domain you are analyzing. With luck, you were able to collect information about the numbers and sophistication levels of the hackers who operate from the attacking domain, possible candidates for the attack (through finger or specialized Altavista searches), and what other CERTs may be seeing from that domain (via newsgroups or newswire searches). An excellent site to check for archived postings of recently seen attacks is both *http://www.sans.org* and *http://www.securityfocus.com*. Ask yourself, were there thousands of hacker pages hosted on the domain that you were investigating? Likewise, did you find thousands of postings concerning hacking on USENET? Did you run a search on your organization's name plus "hack*"? Were there postings from other administrators detailing attacks from this domain? Were the attacks they mentioned similar to yours or different? Now you might be able to determine if that FTP probe, for example, was just a random probe that targeted several other companies as well as yours or targeted your company specifically. Could you tell from the logs that the attacker was attempting to find a vulnerable FTP server to perhaps set up a warez or mp3 site? Being able to make an educated guess about the motivation of your hacker is important. Knowing whether your company has been singled out for an attack as opposed to being randomly selected will change the level of concern you have about assessing the threat. The process previously outlined can be used to narrow down possible candidates or characterize the threat level from responsible domains. As a byproduct, it will also provide you with all the necessary names, phone numbers, and points of contact that may be useful when it comes time to notify the pertinent parties involved.

Finally, let's look at what is probably the most important computer forensics service: training. It has now been expanded to support U.S. government and U.S. corporate needs, which became more of a priority after September 11, 2001. It places priority on computer incident responses and now covers computer forensic binary data searches for foreign language (non-Latin based) computer data (Farsi, Chinese, Japanese, etc.).

Training

As previously explained, computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored in the form of magnetically encoded information (data). Often the computer evidence was created transparently by the computer's operating system and without the knowledge of the computer operator. Such information may actually be hidden from view and, thus, special forensic software tools and techniques are required to preserve, identify, extract, and document the related computer evidence. It is this information that benefits law enforcement and military agencies in intelligence gathering and in the conduct of investigations.

Today computer forensics software tools and processing techniques have become important resources for use in internal investigations, legal electronic document discovery, computer security risk management, and computer incident responses. Computer forensic software tools and methods can be used to identify passwords, computer network log-ons, and other information that is transparently and automatically transferred from the computer's memory to floppy diskettes, Iomega Zip Disks, and computer hard disk drives. Such computer forensic software tools and methods can also be used to identify backdated files and to tie a floppy diskette to a specific computer. These techniques should be taught in your specialized training course.

Law enforcement and military agencies have been involved in processing computer evidence for years. Therefore, computer forensics training courses should be taught by certified instructors (see sidebar, "Computer Forensics Certified") who are experienced computer crime experts (retired federal law enforcement computer evidence trainers and members of law enforcement computer crime units).

COMPUTER FORENSICS CERTIFIED

According to a Gartner Group study, certification of INFOSEC computer-forensic-training professionals is becoming a common condition of employment. The research firm predicts that by 2009, INFOSEC certification will be required for 90% of CISOs (chief information security officers) and associated training staff positions and for 70% of day-to-day technical operations positions in Global 2004 companies. Security is the number one issue going forward in an online world, whether it's online voting or e-commerce.

THE DEMANDS OF SECURITY

It's bad enough when a certified IT employee doesn't possess claimed skills, but the skills gap is doubly worse in the security realm. What was once the near-exclusive purview of government agencies or companies involved in highly secret research is now a mainstream discipline for the highly connected enterprise.

This market didn't exist 13 years ago. The field has only matured in the past 6 years.

Protecting a company's most cherished assets (not just IT systems, but especially the digitally stored proprietary information on those systems) demands knowledgeable personnel, something not always easy to assess. Anyone can hang out a shingle and say: "I'm an INFOSEC professional." Such people must be able to prove their credentials with INFOSEC certification.

Good security demands a more proactive approach than the other traditional functions of a system administrator. Security is the system administrator area that requires the most constant learning and relearning.

Information security infrastructure, like the proverbial chain, is only as strong as its weakest link. The breadth of skills and management ability required for strong information security puts unusual demands on organizations and professionals.

ANOTHER GAME

A certified information systems security professional (CISSP) isn't the only game in town. There's also Certified Internet Webmaster (CIW) professional certification, coming on strong.

Perhaps the best known security certification player is the System Administration, Networking, and Security (SANS) Institute, which sponsors the Global Information Assurance Certifications (GIAC). This is where the line in the security sand is drawn. The CISSP is a broad top-down certification, whereas the LevelTwo GIAC is a series of specialized and technical certifications.

→

GIAC responds directly to the skills question. GIAC requires that candidates demonstrate content mastery before they sit for the exam. In intrusion detection, for example, a candidate must accurately analyze ten real-world intrusion attempts before being allowed to take the exam. For firewalls, a candidate must design a perimeter that solves specific problems.

When comparing CISSPs to GIAC, the metaphor is an MBA (CISSP) versus a CPA (GIAC). You hire a CPA to do your accounting but not to do your strategic business planning. Research indicates that strategic business planning is what the industry desperately needs. The principal difference is in the target. An analogy suggested by an International Steering Committee (ISC) board member is that GIAC is for pilots and CISSP is for the managers who schedule the pilots.

SANS certification focuses on specific products. The product focus has limitations, because security professionals need to take into account the whole picture.

The short-term need is for the techie approach. Believe it or not, issues such as buffer overflows still form a large part of the action on security lists. In the long term, though, you need the big-picture view.

You cannot really say the technical issues are more important than management issues, but the technical issues are more solvable.

Indeed, whether approaching information security issues from a management or technical perspective, no one can escape political issues. Even if you had the best of the best techies on your payroll, you wouldn't be going anywhere unless the issues and policies around corporate standards, user awareness, remote and wireless access policies [8], acceptable authentication methods, and so forth have been decided. The critical success factors in most security jobs are being adept at the politics, possessing business skills and aptitude, good relationship management, and sales and negotiation skills, even in some lower-level jobs.

The product versus politics dilemma will eventually be moot with SANS' Security Essentials (LevelOne) certification. The basic GIAC certification now covers all the key knowledge sets covered by CISSP as well as additional, more current skills sets.

Growing a Profession

The information security profession draws people from diverse backgrounds into a cohesive group. Security pros may have backgrounds in law enforcement, the military, or traditional IT, each bringing their own jargon and argot. How do we learn to talk to each other? You need an agreed-on taxonomy, and that, certification advocates indicate, is what certification does: it creates a shared body of knowledge to encourage a cohesive professional body.

→

Such certification is also seen as a big asset to an employee's resume. CISSP is the gold standard of security management and program development, but a certification should be the beginning of a learning process, not an end in itself. Security is one area where yesterday's knowledge does not help. The security threat is always changing, so security certification tests, more than any others, are out of date before the person even begins to study for them.

There's another problem: the SAT-prep-test phenomenon. Once certifications become widely accepted, some of their value will be lost. The more popular something is, the more likely there will be a "for dummies" approach.

Although most computer forensics training courses do not answer all possible questions regarding computer evidence and computer security, they should cover most of the common issues and expose the participant to new state-of-the-art computer forensics techniques and computer forensics tools. Training should consist of a Windows NT computer forensics course and a restricted-data-hiding course. An expert witness testimony on electronic evidence course should fill in the gaps when the participant is ready for those advanced training courses. Training should not be focused on one specific computer forensics software tool or set of tools. This should not be a computer forensics paint by numbers training course. Quality computer forensic software tools should be provided with the training course, but it should be your company's mission to teach methodologies and the more technical aspects of computer evidence processing and computer incident responses.

The training course should be unique; the participants are expected to have a high degree of computer proficiency, know the difference between clusters and sectors, and have experience in the use of latest Microsoft Windows platforms. The course should not be an overview of computer forensics. It should be a technical hands-on training course that will tax your knowledge and computer skills. It should provide you with more information about computer security risks and evidence-processing information than can be found anywhere else.

Because the course should deal with computer security issues and computer risk management as well as computer evidence issues, it should be well suited for computer security specialists, computer incident response team members, and computer crime investigators. Most of your participants should be challenged by this course for it to be considered a success.

NOTE

In special cases, a course like this should be taught at the training facilities of corporate and government sponsors.

COURSE CONTENT

A typical computer forensics course should deal specifically with Windows 2000, Windows XP, Windows 2003, and Windows ME. Concerning these operating systems, it should cover evidence preservation, evidence-processing methodologies, and computer security risk assessments in detail. It should touch briefly on issues dealing with Windows NT, Windows 2000, and Windows XP and 2003. However, you should have an advanced Windows NT training course that covers computer security and computer evidence issues associated with Windows NT, Windows 2000, Windows XP, and Windows 2003 in great detail.

Today, Windows XP and Windows 2003 are the predominant operating systems used on notebook and desktop computers. Thus, they are the most likely operating systems to be encountered in computer investigations, internal audits, and computer security reviews. Most computer forensics courses do not cover the use of black box computer forensics software tools. Those tools are good for some basic investigation tasks, but they do not offer a complete and accurate computer forensics solution. Furthermore, such approaches are useless in computer security risk assessments. Computer security risk assessments usually require that searches and file listings be conducted overtly (or covertly) from a single floppy diskette.

Each participant in a computer forensics course who successfully completes the course should receive some sort of certificate of completion that is suitable for framing. They should also leave the course with a good understanding of the following:

- Computer evidence processing
- Preservation of evidence
- Trojan horse programs
- Computer forensics documentation
- File slack
- Data-hiding techniques
- Internet-related investigations
- Dual-purpose programs
- Text search techniques
- Fuzzy logic tools used to identify previously unknown text
- Disk structure
- Data encryption
- Matching a floppy diskette to a computer
- Data compression
- Erased files
- Internet abuse identification and detection
- The boot process and memory resident programs

Computer-Evidence-Processing Procedures

The processing procedures and methodologies taught in a computer forensics course should conform to federal computer-evidence-processing standards. The tools that are used in the course, as well as the methods and procedures taught, should work with any computer forensics tools. The methods and many of the software tools should conform specifically to the computer-evidence-processing procedures followed by the FBI, U.S. Department of Defense, and the U.S. Drug Enforcement Administration.

Preservation of Evidence

Computer evidence is very fragile and it is susceptible to alteration or erasure by any number of occurrences. The participant should be exposed to bit stream back-up procedures that ensure the preservation of all storage levels that may contain evidence.

Trojan Horse Programs

The need to preserve the computer evidence before processing a computer will be clearly demonstrated through the use of programs designed to destroy data and modify the operating systems. The participant should demonstrate his or her ability to avoid destructive programs and traps that can be planted by computer users bent on destroying data and evidence. Such programs can also be used to covertly capture sensitive information, passwords, and network logons. This should also be demonstrated during the course.

Computer Forensics Documentation

The documentation of forensic-processing methodologies and findings is important. This is even true for computer security risk assessments, computer incident responses, and internal audits, because without proper documentation it is difficult to present findings in court or to others. If the computer security or internal audit findings become the object of a lawsuit or a criminal investigation, then accurate documentation becomes even more important. The participant should be taught computer-evidence-processing methodology that facilitates good evidence-processing documentation and solid evidence chain of custody procedures. The benefits will be obvious to investigators, but they will also become clear to internal auditors and computer security specialists during the course.

File Slack

The occurrence of random memory dumps in hidden storage areas [9] should be discussed and covered in detail during workshops. Techniques and automated tools used to capture and evaluate file slack should be demonstrated in the course. Such data is the source of potential security leaks regarding passwords, network logons, email, database entries, and word processing documents. These security and evidence issues should be discussed and demonstrated during the course. The participants should be able to demonstrate their ability to deal with slack from both an investigations and security risk standpoint. They should also be able demonstrate their proficiency in searching file slack, documenting their findings, and eliminating security risks associated with file slack.

Data-Hiding Techniques

Trade secret information and other sensitive data can easily be secreted using any number of techniques. It is possible to hide diskettes within diskettes and to hide entire computer hard disk drive partitions. These issues should be discussed from a detection standpoint as well as from a security risk standpoint. Tools that help in the identification of such anomalies should demonstrated and discussed (AnaDisk). Participants should be required to demonstrate their understanding of such issues. This aspect of the training becomes especially important during the last day of the course when the participants are called on to identify and extract their Certificate of Completion from a *special* floppy diskette.

NOTE

Data-hiding issues should be covered in much more depth in a data-hiding course.

Internet-Related Investigations

Issues and techniques related to the investigation of Internet-related matters should be covered in the course. This should include a demonstration of how Internet-related evidence differs from more traditional computer evidence. Emphasis should be placed on the investigation of Internet-based terrorist leads.

Dual-Purpose Programs

Programs can be designed to perform multiple processes and tasks at the same time. They can also be designed for delayed tasks and processes. These concepts should be demonstrated to the participants during the course through the use of specialized software. The participants should also have hands-on experience with such programs.

Text Search Techniques

Specialized search techniques and tools should be developed that can be used to find targeted strings of text in files, file slack, unallocated file space, and Windows swap files. Each participant should leave the class with the necessary knowledge to conduct computer security reviews and computer-related investigations. Because of the need to search for non-Latin words and word patterns tied to foreign languages, the course should also cover the search of such data tied to foreign languages (Farsi, Chinese, Japanese, etc.).

Fuzzy Logic Tools Used to Identify Previously Unknown Text

A methodology and special computer forensics tools should be developed that aid in the identification of relevant evidence and *unknown* strings of text. Traditional computer evidence searches require that the computer specialist know what is being searched for. However, many times not all is known in investigations. Thus, not all is known about what may be stored on a targeted computer system. In such cases, fuzzy logic tools can assist and can provide valuable leads as to how the subject computer was used. The participants should fully understand these methods and techniques. They should also be able to demonstrate their ability to use them to identify leads in file slack, unallocated file space, and Windows swap files.

Disk Structure

Participants should leave the course with a solid understanding of how computer hard disks and floppy diskettes are structured and how computer evidence can reside at various levels within the structure of the disk. They should also leave the class with a good understanding of how easy it is to modify the disk structure and to hide computer data in obscure places on floppy diskettes and hard disk drives.

Data Encryption

A computer forensics training course should also cover how data is encrypted and illustrate the differences between good encryption and bad encryption. The participants should become familiar with the use of software to *crack* security associated with these different encryption file structures.

Matching a Floppy Diskette to a Computer

Specialized computer forensics techniques and computer forensics tools should also be developed that make it possible to conclusively tie a floppy diskette to a computer hard disk drive. Each participant should also be taught how to use special software tools to complete a unique computer storage data-matching process. Some computer forensics experts believe floppy diskettes are no longer popular. They are wrong. Floppy diskettes are found to be a valuable source of computer evidence in some civil litigation cases that involve the theft of trade secrets.

Data Compression

The participant should be shown how data compression programs can be used to hide and disguise critical computer data. Furthermore, the participant should learn how password-protected compressed files can be broken.

Erased Files

Participants should be shown how previously erased files can be recovered using computer forensics processes and methods. Documentation of the process should also be covered in detail.

Internet Abuse Identification and Detection

The participant should be shown how to use specialized software to identify how a targeted computer has been used on the Internet. This process should focus on computer forensics issues tied to data that the computer user probably doesn't realize exists (file slack, unallocated file space, and Windows swap files). Participants should get hands-on experience in using this unique technology and they should be given the opportunity to purchase the software for a nominal charge. Nevertheless, it should be provided free of charge to law enforcement computer crime specialists who attend the course. Law enforcement agencies are typically underfunded.

The Boot Process and Memory Resident Programs

Participants should be able to see how easy it is to modify the operating system to capture data and to destroy computer evidence. Such techniques could be used to covertly capture keyboard activity from corporate executives, government computers, and the like. For this reason, it is important that the participants understand these potential risks and how to identify them.

Finally, let's look at computer forensics case study scenarios. These scenarios will briefly cover planned forensics responses. Additional case studies and projects may be found at the end of this chapter.

CASE HISTORIES

The following case study illustrates the organizational benefits of a planned forensic response.

Scenario One

An IT manager reviews a detection tool report that indicates a company employee is accessing restricted Internet sites and downloading objectionable material. After discovering the activity, the IT manager remotely accesses the employee's personal computer to obtain evidence. The employee is then dismissed, based on the evidence located and obtained.

Scenario Two

An IT manager reviews a detection tool report indicating a company employee is accessing restricted Internet sites and downloading objectionable material. After discovering this activity, the IT manager follows procedures, reporting his suspicions to the nominated computer incident response contact, in this case the chief information officer (CIO).

The CIO then invokes the company's incident response plan by contacting the incident response team, which includes computer forensics experts. This team isolates the *offending machine;* conducts a forensic examination of the computer system following methodologies known to be acceptable to criminal, civil, and arbitration courts or tribunals; and establishes where the material came from, how often, and who else knew about it. By following its effective policies and procedures, the organization (via the CIO) is in an excellent position to take immediate legal and decisive action based on all the available facts and evidence.

Which Scenario Works?

Only one of these scenarios illustrates a planned forensic response. In Scenario One, the evidence was obtained remotely. This fact alone may put the obtained evidence in doubt.

Any court of law would want to know whether there were policies and IT infrastructure for ensuring the IT staff member knew the correct PC was accessed. Other issues surround the need for evidence to prove that a particular employee's PC was responsible for downloading the objectionable material. Can it be proved that the objectionable material was viewed on a particular PC? Who else had access to that PC? It is likely that there is not adequate evidence in this scenario to answer these questions.

The IT manager detecting activity is only the first step in forming grounds for suspicion. If action is taken without proper policies, procedures, and processes in place, it is nothing more than an unplanned knee jerk reaction.

Unplanned reactions potentially expose an organization to risk. Clearly, any investigation must not only be thorough and methodical, but also staffs need procedures for reporting the activity, conducting the investigation, and appointing investigators.

Finally, in Scenario Two, the established policies let the organization clearly identify the incident and carry out appropriate immediate action. This places the organization in a comfortable position to resolve the situation, contain the potential damage, and effectively seek compensation or prosecution. The bottom line here is that without the appropriate procedures in place to counter detected attacks, an organization is exposed to the risks of lost data, financial loss, network damage, and loss of reputation.

SUMMARY

Don't react. Respond. Cyber crime is rapidly increasing and is striking at the heart of many organizations. By ensuring measures such as effective policies and rapid response capabilities, excellent information technology security positioning and forensic support can exist. Businesses can respond quickly, minimizing the risks of lost data, financial loss, network damage, and loss of reputation.

Organizations wanting to counter cyber crime need to apply risk management techniques that allow a speedy response and minimize harm. Although organizations cannot prevent a cyberattack, they can have a planned response and even turn e-crime preparedness, or effective security, into a new competitive advantage.

Conclusions

- The technological revolution marches on at a frantic pace, providing the world with an immense availability of resources. The same technological revolution has also brought forth a new breed of investigative and legal challenges.
- Computers are now at the core of people's activities, and evidence contained in them is being introduced with greater frequency in both civil and criminal judicial proceedings. Questions arise regarding location of evidence stored on digital media, analysis of that evidence, and authentication of that evidence in court. The field of computer forensics seeks to answer these questions and provide experts to introduce this digital evidence in court.
- Computer forensic services include digital evidence collection, forensic analysis of digital evidence (including analysis of hidden, erased, and password-protected files), expert witness testimony. and litigation support.
- Who can benefit from computer forensic services: attorneys involved in complex litigation that deals with digital evidence; human resource professionals involved in administrative proceedings such as wrongful termination claims, sexual harassment, discrimination allegations, and employee violations of company policies and procedures, where key evidence may reside in emails, word processing documents, and the like; and company executives who are interested in confidentially auditing their employees' computer usage concerning proprietary information, misuse of company resources, and trade secret issues.

- Insurance companies are interested in reducing fraudulent claims by using discovered digital evidence.
- Documentary evidence has quickly moved from the printed or type-written page to computer data stored on floppy diskettes, zip disks, CDs, and computer hard disk drives.
- Denial of service attacks have always been difficult to trace as a result of the spoofed sources.
- With the recent increasing trend toward using distributed denial of service attacks, it has become near impossible to identify the true source of an attack.
- ISPs need automated methods as well as policies in place to attempt to combat the hacker's efforts.
- Proactive monitoring and alerting of backbone and client bandwidth with trending analysis is an approach that can be used to help identify and trace attacks quickly without resource-intensive side effects.
- Subsequent detailed analysis could be used to complement the bandwidth monitoring.
- Timely communication between ISPs is essential in incident handling.
- Deleted computer files can be recovered.
- Even after a hard drive is reformatted or repartitioned, data can be recovered.
- In many instances, encrypted files can be decrypted.
- Forensic analysis can reveal what Web sites have been visited, what files have been downloaded, when files were last accessed, when files were deleted, attempts to conceal or destroy evidence, and attempts to fabricate evidence.
- The electronic copy of a document can contain text that was removed from the final printed version.
- Some fax machines can contain exact duplicates of the last several hundred pages received.
- Faxes sent or received via computer may remain on the computer indefinitely.
- Email is rapidly becoming the communications medium of choice for businesses. People tend to write things in email that they would never consider writing in a memorandum or letter. Email has been used successfully in civil cases as well as criminal cases, and email is often backed up on tapes that are generally kept for months or years.
- Many people keep their financial records, including investments, on computers.

An Agenda for Action

When completing the Vender and Forensic Services Types Checklist (as shown in Table F4.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for some of the principle types of vendor and computer forensics services. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Cyber crime occurs when information technology is used to commit or reveal an offense.
2. True or False? Forensic investigators detect the extent of a security breach, recover lost data, determine how an intruder got past security mechanisms, and, potentially, identify the culprit.
3. True or False? The best approach for organizations wanting to counter cyber crime is not to apply risk-management techniques.
4. True or False? There are without doubt some very good experts in the field of computer forensics investigations; however, there is a rise in the number of people purporting to be experts or specialists who produce flawed opinions or take actions that are just plain wrong.
5. True or False? The risk any system connected to the Net faces is a product of vulnerability and threat.

Multiple Choice

1. Computer crimes include the following, except:
   A. Financial information
   B. Sabotage of data and/or networks
   C. Theft of proprietary information
   D. System penetration from the outside and denial of service
   E. Unauthorized access by insiders and employee misuse of Internet access privileges

2. The following are some helpful tips that you can follow to help preserve data for future computer forensic examination, except:
   - A. Do not turn on or attempt to examine the suspect computer. This could result in destruction of evidence.
   - B. Identify all devices that may contain evidence.
   - C. Run all in-house computers.
   - D. Quarantine all in-house computers.
   - E. Forensically image all suspect media.
3. Each participant in a computer forensics course who successfully completes the course should receive some sort of a certificate of completion that is suitable for framing. They should also leave the course with a good understanding of the following, except:
   - A. Computer evidence processing
   - B. Preservation of evidence
   - C. Troy horse programs
   - D. Computer forensics documentation
   - E. File slack
4. Internal events are committed by those with a substantial link to the intended victim, for example, a bank employee who siphons electronic funds from a customer's account. Other examples include the following, except:
   - A. Downloading or distributing offensive material
   - B. Theft of intellectual property
   - C. Internal system intrusions
   - D. Fraud
   - E. Unintentional or intentional addition or damage of data or systems
5. Forensic investigators perform the following, except:
   - A. Detect the extent of a security breach.
   - B. Recover found data.
   - C. Recover lost data.
   - D. Determine how an intruder got past security mechanisms.
   - E. Potentially, identify the culprit.

Exercise

Following a technical investigation of embezzlement at an insurance company, a CFS was engaged by the company's general counsel to perform data sweeping services to help mitigate digital evidence liabilities. How would the CFS handle this analysis?

HANDS-ON PROJECTS

Data Recovery Services in Action

After two former employees left a high-quality large-format imaging firm to work for a competitor, the defendants emailed the firm's customer database to their home computer in an attempt to steal intellectual property from the firm and provide it to their new employer. They firmly denied the allegations put forth by the firm, believing that no one would find out since they had deleted the email and the attachment containing the customer database from their home computer. How would the firm's CFS team go about investigating this case?

Case Projects

A large computer services corporation suspected an employee, who was a foreign national, of hacking into other classified computer systems based on information generated by the corporation's external auditing software program. How would a CFS team go about investigating this incident?

Optional Team Case Project

After finding pornography downloaded on its network server and a number of individual office computers, a company began to build a case for employee dismissal. Explain the company's solution in detail regarding the organization's investigation into this matter.

REFERENCES

[1] "Computer Forensics: Response Versus Reaction," Ernst & Young Australia, The Ernst & Young Building, 321 Kent Street, Sydney NSW 2000, Australia (Ernst & Young LLP, 787 Seventh Avenue, New York, New York, 10019), 2001, p.3.

[2] "2003 Computer Crime and Security Survey," Federal Bureau of Investigation, J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW, Washington, D.C. 20535-0001, 2003.

[3] Vacca, John R., *Electronic Commerce: Online Ordering and Digital Money*, Charles River Media, Hingham, MA, 2001.

[3a] Federal Bureau of Investigation, J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW, Washington, D.C. 20535-0001, 2003.

[4] Vacca, John R., *Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan*, McGraw-Hill Professional, New York, 2001.

[5] Katherine Bursese, "Computer Security Incident Response Procedures: Do You Need One? You Bet You Do!" Global Computer Operations, General Electric Company, 2690 Balltown Road, Bldg. 610, Schenectady, NY 12345 (SANS Institute, 5401 Westbard Ave. Suite 1501, Bethesda, MD 20816), 2002.

[6] Vacca, John R., *Planning, Designing, and Implementing High-Speed LAN/WAN with Cisco Technology*, CRC Press, Boca Raton, FL, 2002.

[7] "Computers," Rehman Technology Services, Inc., 18950 U.S. Highway 441, #201, Mount Dora, Florida 32757, 2001.

[8] Vacca, John R., *Wireless Broadband Networks Handbook*, McGraw-Hill Professional, New York, 2001.

[9] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

This page intentionally left blank

Part II

Computer Forensics Evidence and Capture

The second part of this book discusses data recovery, evidence collection and data seizure, duplication and preservation of digital evidence, and computer image verification and authentication.

This page intentionally left blank

5 Data Recovery

Computers systems may crash. Files may be accidentally deleted. Disks may accidentally be reformatted. Computer viruses may corrupt files. Files may be accidentally overwritten. Disgruntled employees may try to destroy your files. All of these can lead to the loss of your critical data. You may think it's lost forever, but you should employ the latest tools and techniques to recover your data.

In many instances, the data cannot be found using the limited software tools available to most users. The advanced tools should allow us to find your files and restore them for your use. In those instances where the files have been irreparably damaged, your computer forensics expertise should allow you to recover even the smallest remaining fragments.

Data recovery is, of course, of potential interest to anyone who has lost data to the ravages of time, malice, or carelessness, but in forensic computing or analysis, it takes on a new meaning—suddenly what other people have thrown away can become an important component in understanding what has happened in the past, as burglary tools, data files, correspondence, and other clues can be left behind by interlopers.

This chapter covers the ins and outs of data recovery as it relates to computer forensics, but before delving into the ins and outs, what is data recovery?

DATA RECOVERY DEFINED

Data recovery is the process in which highly trained engineers evaluate and extract data from damaged media and return it in an intact format. Many people, even computer experts, fail to recognize data recovery as an option during a data crisis, yet it is possible to retrieve files that have been deleted and passwords that have been forgotten or to recover entire hard drives that have been physically damaged.

As computers are used in more important transactions and storage functions, and more important data is stored on them, the importance of qualified data recovery experts becomes clear. Perhaps your information has been subjected to a virus attack, suffered damage from smoke or fire, or your drive has been immersed in water—the data recovery experts can help you. Perhaps your mainframe software has malfunctioned or your file allocation tables are damaged—data recovery experts can help you.

What would happen to the productivity of your organization in the event of a system-wide data center failure? For most companies, the loss would be catastrophic. Hundreds, perhaps thousands, of employees would be rendered unproductive. Sales transactions would be impossible to complete and customer service would suffer. The cost of replacing this data would be extraordinary—if it could be replaced at all.

DATA BACKUP AND RECOVERY

You live in a world that is driven by the exchange of information. Ownership of information is one of the most highly valued assets of any business striving to compete in today's global economy. Companies that can provide reliable and rapid access to their information are now the fastest growing organizations in the world. To remain competitive and succeed, they must protect their most valuable asset—data.

Fortunately, there are specialized hardware and software companies that manufacture products for the centralized backup and recovery of business-critical data. Hardware manufacturers offer automated tape libraries that can manage millions of megabytes of backed up information and eliminate the need for operators charged with mounting tape cartridges. Software companies have created solutions that can back-up and recover dozens of disparate systems from a single console.

Why then, do industry experts estimate that over 56% of the data in client/server networks is still not backed up on a regular basis? It is often due to organizations' ever-shrinking back-up windows, inadequate network infrastructure, and a lack of system administration. Compounding the problem is an overall lack of experience in defining the proper features necessary for a successful; backup application. Finally, there is often a shortage of in-house expertise needed to implement sophisticated, enterprise-level backup applications.

Backup Obstacles

The following are obstacles to backing up applications:

- Backup window
- Network bandwidth
- System throughput
- Lack of resources
- Backup Window

The backup window is the period of time when backups can be run. The backup window is generally timed to occur during nonproduction periods when network bandwidth and CPU utilization are low. However, many organizations now conduct operations 7 days a week, 24 hours a day—effectively eliminating traditional backup windows altogether.

Network Bandwidth

Many companies now have more data to protect than can be transported across existing local area networks (LANs) and wide area networks (WANs). If a network cannot handle the impact of transporting hundreds of gigabytes of data over a short period of time, the organization's centralized backup strategy is not viable.

System Throughput

Three I/O bottlenecks are commonly found in traditional backup schemes. These are

1. The ability of the system being backed up to push data to the backup server
2. The ability of the backup server to accept data from multiple systems simultaneously
3. The available throughput of the tape device(s) onto which the data is moved [1]

Any or all preceding bottlenecks can render a centralized backup solution unworkable.

Lack of Resources

Many companies fail to make appropriate investments in data protection until it is too late. Often, information technology (IT) managers choose not to allocate funding for centralized data protection because of competing demands resulting from emerging issues such as e-commerce [2], Internet and intranet applications, and other new technologies.

These are just a few of the impediments that make implementation of an enterprise backup and recovery solution a low priority for some organizations. Fortunately, there have been major advances in hardware and software technologies that overcome many or all of the traditional obstacles faced by IT professionals as they attempt to develop a comprehensive data-protection plan. In addition, companies such as StorNet [3] provide specialized expertise in the deployment of complex, integrated storage solutions.

The Future of Data Backup

Successful data backup and recovery is composed of four key elements: the backup server, the network, the backup window, and the backup storage device (or devices). These components are highly dependent on one another, and the overall system can only operate as well as its weakest link. To help define how data backup is changing to accommodate the issues described earlier, let's take a look at each element of a backup and recovery design and review the improvements being made.

The Backup Server

The backup server is responsible for managing the policies, schedules, media catalogs, and indexes associated with the systems it is configured to back up. The systems being backed up are called *clients*. Traditionally, all managed data that was being backed up had to be processed through the backup server. Conversely, all data that needed to be restored had to be accessed through the backup server as well. This meant that the overall performance of a backup or recovery was directly related to the ability of the backup server to handle the I/O load created by the backup process.

In the past, the only way to overcome a backup server bottleneck was to invest in larger, more powerful backup servers or data backup and recovery and divide the backup network into smaller, independent groups. Fortunately, backup-software developers have created methods to work around these bottlenecks. The most common workaround is to create *tape* servers that allow administrators to divide the backup tasks across multiple systems while maintaining scheduling and administrative processes on a primary or *backup* server. This approach often involves attaching multiple tape servers to a shared tape library, which reduces the overall cost of the system. Figure 5.1 is an example of a backup configuration such as this [3].

The newest backup architecture implements a serverless backup solution that allows data to be moved directly from disk to tape, bypassing the backup server altogether. This method of data backup removes the bottleneck of the backup server completely. However, the performance of serverless backup is then affected by another potential bottleneck—bandwidth. Figure 5.2 is an example of a serverless backup [3].

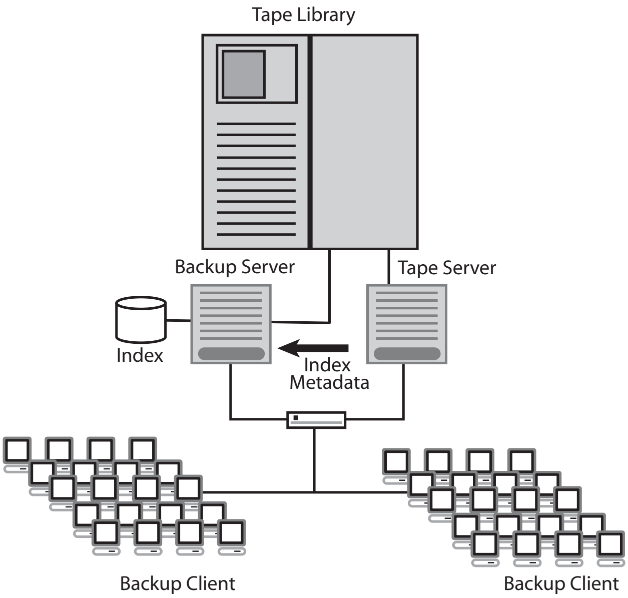


FIGURE 5.1 A backup using a shared tape library. (© Copyright 2002, StorNet. All rights reserved.)

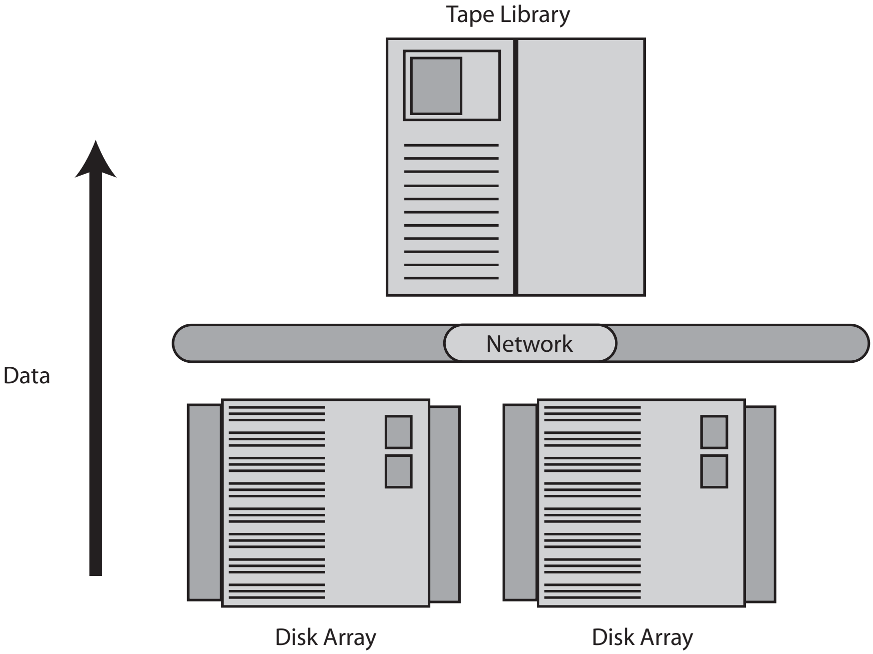


FIGURE 5.2 A serverless backup system. (© Copyright 2002, StorNet. All rights reserved.)

The Network Data Path

Centralization of a data-management process such as backup and recovery requires a robust and available network data path. The movement and management of hundreds or thousands of megabytes of data can put a strain on even the best-designed networks. Unfortunately, many companies are already struggling with simply managing the existing data traffic created by applications such as e-commerce, the Internet, email, and multimedia document management. Although technology such as gigabit Ethernet and asynchronous transfer mode (ATM) can provide relief, it is rarely enough to accommodate management of large amounts of data movement.

If there is not enough bandwidth to move all the data, what are the options? Again, it was the backup-software vendors who developed a remedy. An enterprise-class backup solution can distribute backup services directly to the data source, while at the same time centralizing the administration of these resources. For example, if there is a 600-gigabyte database server that needs to be backed up nightly, a tape backup device can be attached directly to that server. This effectively eliminates the need to move the 600-gigabyte database across the network to a centralized backup server. This approach is called a LAN-less backup, and it relies on a remote tape server capability. Figure 5.3 demonstrates how this approach is configured [3].

Another option is the installation of a network path dedicated to the management and movement of data. This data path can be SCSI, Ethernet, ATM, fiber distributed data interface (FDDI), or fibre channel. Creating a dedicated data path is the beginning of a storage area network (SAN) [4]. SANs are quickly dominating the backup landscape, and applications such as serverless and LAN-less backup will continue to push this emerging technology forward. Figure 5.4 shows an example of a dedicated SAN topology [3].

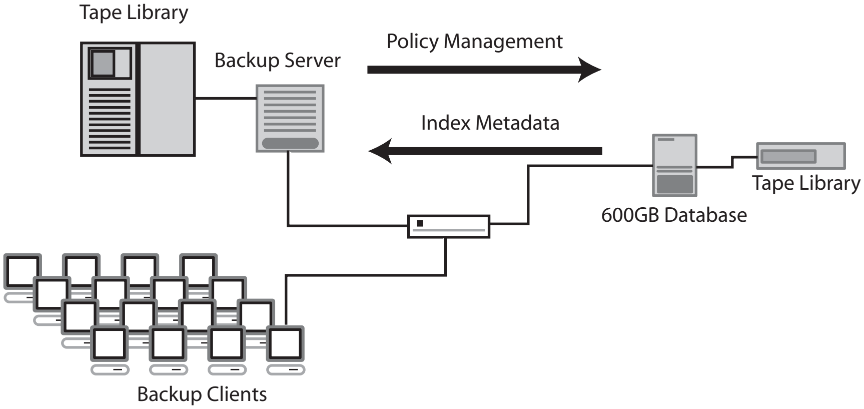


FIGURE 5.3 A LAN-less back-up using a remote tape server. (© Copyright 2002, StorNet. All rights reserved.)

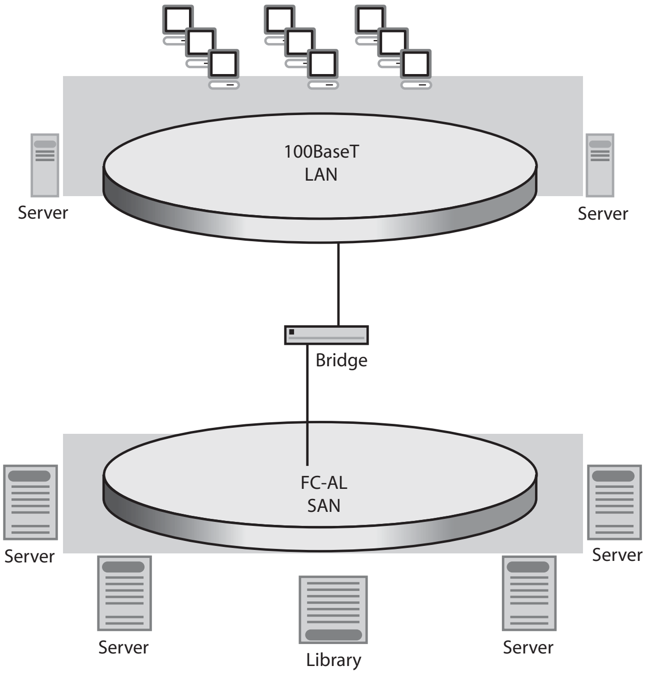


FIGURE 5.4 A storage area network using serverless backup. (© Copyright 2002, StorNet. All rights reserved.)

The Backup Window

Of all the parameters that drive the design of a backup application, one remains an absolute constant, and that is time. A backup window defines how much time is available to back up the network. Time plays an important role in choosing how much server, network, and resource support needs to be deployed. Today, most companies are managing too much data to complete backup during these ever-shrinking backup windows.

In the past, companies pressured by inadequate backup windows were forced to add additional backup servers to the mix and divide the backup groups into smaller and smaller clusters of systems. However, the backup-software community has once again developed a way to overcome the element of time by using incremental backup, block-level backup, image backups, and data archiving.

Incremental Backup

Incremental backups only transfer data that has changed since the last backup. On average, no more than 5% of data in a file server changes daily. That means an incremental backup may only require 5% of the time it takes to back up the entire file system. Even then, a full backup had to be made regularly, or restoration of the data would take too long. Fortunately, there are now backup applications that combine incremental backups, thereby creating a *virtual* complete backup every night without necessitating a full backup during the limited backup window.

Block-Level Incremental Backup

Block-level incremental backups provide similar benefits as incremental backups, but with even more efficiency. Rather than backing up entire files that have been modified since the last backup, only the blocks that have changed since the last backup are marked for backup. This approach can reduce the amount of incremental data requiring backup nightly by orders of magnitude.

However, this benefit comes at a price. Often the file system of the client must be from the same vendor as the backup software. Also, there are databases such as Oracle that allow block-level backups, but the CPU requirements to do so may render the approach ineffective. Nevertheless, block-level backups may be the only viable option for meeting your backup window.

Image Backups

Image backups are quickly gaining favor among storage administrators. This type of backup creates copies, or *snapshots,* of a file system at a particular point in time. Image backups are much faster than incremental backups and provide the ability to easily perform a *bare bones* recovery of a server without loading the operating systems, applications, and the like. Image backups also provide specific point-in-time backups that can be done every hour rather than once a day.

Data Archiving

Removing infrequently accessed data from a disk drive can reduce the size of a scheduled backup by up to 80%. By moving static, infrequently accessed data to tape, backup applications are able to focus on backing up and recovering only the most current and critical data. Static data that has been archived is easily recalled when needed but does not add to the daily data backup requirements of the enterprise. This method also provides the additional benefit of freeing up existing disk space without adding required additional capacity.

Backup Storage Devices

In many cases, the single most expensive item in a backup project is the backup storage device itself. Therefore, it is important that the technical specifications of the storage device provide adequate capacity and performance to accommodate existing and planned data. Determining the tape format, number of tape drives, and how many slots are required is predicated on many variables. Backup windows, growth rates, retention policies, duplicate tape copies, and network and server throughputs all affect which backup storage device is best for your needs.

Tape libraries are sized using two variables: the number of tape drives and the number of slots; manufacturers of tape libraries continue to improve each of these elements. Tape libraries today are available with 5 to 50,000 slots and can support anywhere from 1 to 256 tape drives. Additionally, there are tape libraries available that support multiple tape formats.

When designing a centralized data backup, take particular care selecting the right backup storage device. Make sure it can easily scale as your data rates increase. Verify that the shelf life of the media meets your long-term storage needs. Calculate the required throughput to meet your backup window and make sure you can support enough tape drives to meet this window.

Recommended Backup Features

Today's global economy means that applications such as email, relational databases, e-commerce, and enterprise resource planning (ERP) systems must be accessible and online 24 hours a day. Therefore, these applications cannot be shut down to perform administrative tasks such as backup. A backup vendor should provide agents for the most common database and email applications that allow these databases to be backed up without shutting down applications.

Data Interleaving

To back up multiple systems concurrently, the backup application must be able to write data from multiple clients to tape in an interleaved manner. Otherwise, the clients must be backed up sequentially, which takes much longer.

Remote Backup

Many remote systems are exposed to unrecoverable data loss. Off-site locations are often not backed up at all because of the cost of deploying hardware and software remotely and the lack of administrative support in these remote locations. Laptop computers are especially vulnerable to data loss. A backup application should have a method to back up systems across a WAN or over dial-up connections.

Global Monitoring

Companies are deploying applications that can be managed and monitored from any location in the enterprise. Backup applications also need to be able to be accessed and administered from multiple locations. A robust backup application should be able to support reporting and administration of any backup system, regardless of location.

Performance

An enterprise backup application should be able to benchmark backup data rates exceeding one terabyte per hour. These benchmarks show that backup performance is limited to the hardware and network and not to the application itself.

Now, let's explore some of the issues concerning the role of backup in data recovery and some of the technologies that are available today. Then, let's take a look at what is still missing in the race to address fast recovery of these exponentially growing data repositories.

THE ROLE OF BACKUP IN DATA RECOVERY

Many factors affect back-up:

- Storage costs are decreasing.
- Systems have to be online continuously.
- The role of backup has changed.

Storage Costs Are Decreasing

The cost per megabyte of primary (online) storage has fallen dramatically over the past several years and continues to do so as disk drive technologies advance. This has a huge impact on backup. As users become accustomed to having immediate access to more and more information online, the time required to restore data from secondary media is found to be unacceptable.

Systems Have to Be Online Continuously

Seven/twenty-four (7 × 24) operations have become the norm in many of today's businesses. The amount of data that has to be kept online and available (operationally ready data) is very large and constantly increasing. Higher and higher levels of fault tolerance for the primary data repository is a growing requirement. Because systems must be continuously online, the dilemma becomes that you can no longer take files offline long enough to perform backup.

The Role of Backup Has Changed

It's no longer just about restoring data. Operationally, ready or *mirrored* data does not guard against data corruption and user error. The role of backup now includes the responsibility for recovering user errors and ensuring that *good* data has been saved and can quickly be restored.

Conventional Tape Backup in Today's Market

Current solutions offered by storage vendors and by backup vendors focus on network backup solutions. To effectively accomplish backup in today's environment, tape management software is generally bundled with several other components to provide a *total* backup solution. A typical tape management system consists of a dedicated workstation with the front-end interfaced to the network and the back-end controlling a repository of tape devices. The media server runs tape management software. It can administer backup devices throughout an enterprise and can run continuous parallel backups and restores.

An alternative to tape backup is to physically replicate or mirror all data and keep two copies online at all times. Because the cost of primary storage is falling, this as not as cost-prohibitive as it once was. The advantage is that the data does not have to be restored, so there are no issues with immediate data availability. There are, however, several drawbacks to all the backup and data availability solutions on the market today.

Issues with Today's Backup

Network backup creates network performance problems. Using the production network to carry backup data, as well as for normal user data access, can severely overburden today's busy network resources. This problem can be minimized by installing a separate network exclusively for backups, but even dedicated backup networks may become performance bottlenecks.

Offline backup affects data accessibility. Host processors must be quiescent during the backup. Backup is not host-independent, nor is it nondisruptive to normal data access. Therefore, the time that the host is offline for data backup must be minimized. This requires extremely high-speed, continuous parallel backup of the raw image of the data. Even in doing this, you have only deferred the real problem, which is the time needed to restore the information. Restoration of data needs to occur at the file level, not the full raw image, so the most critical information can be brought back into operation first.

Live backups allow data access during the backup process but affect performance. Many database vendors offer *live* backup features. The downside to the live backup is that it puts a tremendous burden on the host. Redirection lives on the host, and journaling has to occur on the host. This requires consideration of local storage, host CPU cycles, and host operating system dependencies. Up to 50% of all host CPU cycles may be consumed during the backup process, severely impacting performance.

Mirroring doesn't protect against user error and replication of *bad* data. Fully replicated online data sounds great, albeit at twice the cost per megabyte of a single copy of online data. However, synchronizing, breaking, and resynchronizing mirrors is not a trivial process and influences data access speeds while they are occurring. Also, duplicating data after a user has deleted a critical file or making a mirrored copy of a file that has been corrupted by a host process doesn't help. Mirroring has its place in backup and recovery but cannot solve the problem by itself.

New Architectures and Techniques Are Required

Backup at extremely high speed, with host-processor independence of the underlying file structures supporting the data, is required. Recovery must be available at the file level. The time that systems are offline for back-up must be eliminated.

Mirroring, or live data replication for *hot* recovery also has a role. For data that must be always available, highly fault-tolerant primary storage is not enough, nor is a time-consuming backup/restore. Remote hot recovery sites are needed for immediate resumption of data access. Backup of critical data is still required to ensure against data errors and user errors. Backup and mirroring are complementary, not competing technologies.

To achieve effective backup and recovery, the decoupling of data from its storage space is needed. Just as programs must be decoupled from the memory in which they're executed, the stored information itself must be made independent of the storage area it occupies.

It is necessary to develop techniques to journal modified pages, so that journaling can be invoked within the primary storage device, without host intervention. Two separate pipes for file access must be created: one pipe active and the other dynamic. The primary storage device must employ memory-mapping techniques that enable the tracking of all modified information. Two copies of each change must be kept, with a thread composed of all old data stored in the journaled file.

Part of the primary storage area must be set aside for data to be backed up. This area must be as large as the largest backup block (file, logical volume, etc.). The point-in-time *snapshot* of changed data will be used for backup, while the file itself remains in normal operation without impacting user access to data. To minimize this reserve storage area for backups, the storage device must support the reuse of this area by dynamically remapping.

Mechanisms must be put in place to allow for the backup of data to occur directly from the primary storage area to the backup area without host intervention. Host CPU bottlenecks and network bottlenecks are then eliminated. The net result will be faster user response times during *live* backup, normal network performance levels throughout the process, and no backup downtime.

What about restore times? Fast, nonrandom restoration of critical data assumes that the user can select at the file level exactly which information comes back online first. Here again, the primary storage and its backup software must offload that burden from the host and take on the responsibility for understanding the underlying file structures of multiple heterogeneous hosts. The necessary indexing of file structures can be done in the background subsequent to a high-speed backup. Then, at the time of restore, the indices are accessible to allow selection at the file level for the recovery of the information from the backup device.

How achievable is this scenario? Many backup tools are available today. What has been missing are architectures that can support journaling within the primary storage area, to enable direct, *live* backup with high-speed file-level restores. A few storage vendors, mostly in the mainframe arena, provide some of these types of solutions. Thanks to this kind of progress on the part of storage vendors and their back-up partners, techniques to address continuous operations and fast data recovery in today's 7 × 24 business environment are now becoming both more cost-effective and more widely available.

THE DATA-RECOVERY SOLUTION

Availability once meant that an application would be available during the week, from 9 to 5, regardless of whether customers needed anything. Batch processing took over the evenings and nights, and most people didn't care because they were at home asleep or out having fun. But the world has changed. It's now common to offer extended service hours in which a customer can call for help with a bill, inquiry, or complaint. Even if a live human being isn't available to help, many enterprise applications are Web-enabled so that customers can access their accounts in the middle of the night while sitting at home in their pajamas.

Shrinking Expertise, Growing Complexity

Increased availability is good, except for one fact: many systems programmers, database administrators (DBAs), and other mainframe experts are maturing. It takes a lot of *care and feeding* to keep applications ready for work, and the people who have maintained these environments for so long have other things they want to do. Many are starting to shift their sights toward that retirement community in Florida that they've heard so much about. Most of the bright youngsters who are graduating from college this term haven't had much exposure to mainframe concepts in their course work, much less any meaningful grasp of the day-to-day requirements for keeping mainframe systems running.

The complex systems that have evolved over the past 30 years must be monitored, managed, controlled, and optimized. Batch windows are shrinking down to almost nothing. Backups often take place while an application is running. Application changes take place on the fly, under the watchful eye of the change-control police. If an outage occurs, the company stands to lose tens of thousands of dollars an hour. In today's gloomy economy, stockholders don't want to hear that their favorite investment is having system availability problems.

Failures

Certainly, hardware failures were once more common than they are today. Disk storage is more reliable than ever, but failures are still possible. More likely to occur, though, is a simple mistake made by an application programmer, system programmer, or operations person. Logic errors in programs or application of the wrong update at the wrong time can result in a system crash or, worse, an undetected error in the database—undetected, that is, until minutes, hours, or days later when a customer calls, a reconciliation fails, or some other checking mechanism points out the integrity exposure.

Finally, disasters do sometimes strike, and most often they occur without warning. Flooding doesn't always occur when it's convenient; tornadoes never do. Hurricanes and earthquakes are big-ticket events that ruin everyone's day. When they strike your data center, wipe out your processing power, or even destroy your basement-level backup power supply, you have a lot of recovering to do.

Budgets and Downtime

Does anyone need a reminder that budgets are tight? You have fewer resources (people, processing power, time, and money) to do more work than ever before, and you must keep your expenses under control. Shrinking expertise and growing complexity cry out for tools to make systems management more manageable, but the tools that can save resources (by making the most of the ones you have) also cost you resources to obtain, implement, and operate.

Businesses today simply cannot tolerate availability problems, no matter what the source of the problem. Systems must remain available to make money and serve customers. Downtime is much too expensive to be tolerated. You must balance your data management budget against the cost of downtime.

Recovery: Think Before You Back Up

One of the most critical data-management tasks involves recovering data in the event of a problem. For this reason, installations around the world spend many hours each week preparing their environments for the possibility of having to recover. These preparations include backing up data, accumulating changes, and keeping track of all the needed resources. You must evaluate your preparations, make sure that all resources are available in usable condition, automate processes as much as possible, and make sure you have the right kind of resources.

Evaluate Your Preparations

Often the procedures that organizations use to prepare for recovery were designed many years ago. They may or may not have had *care and feeding* through the years to ensure that preparations are still sufficient to allow for recovery in the manner required today.

Here is a simple example: say an organization has always taken weekly image copies on the weekend and has performed change accumulations at mid-week. Will this approach continue to satisfy their recovery requirements? Perhaps. If all of the resources (image copies, change accumulations, and logs) are available at recovery time, these preparations certainly allow for a standard recovery. However, if hundreds of logs must be applied, the time required for the recovery may be many hours—often unacceptable when the cost of downtime is taken into account.

This example illustrates the principle that, although your recovery strategy was certainly adequate when it was designed, it may be dangerously obsolete given today's requirements for increased availability. What if a required resource is damaged or missing? How will you find out? When will you find out? Finding out at recovery time that some critical resource is missing can be disastrous!

Don't Let Your Resources Fall Through the Cracks

The previous example was unrealistically simplistic. Many organizations use combinations of batch and online image copies of various groups of databases, as well as change accumulations, all staggered throughout the week. In a complex environment, how do you check to make sure that every database is being backed up? How do you find out whether you are taking image copies (either batch or online) as frequently as you planned? How do you determine whether your change accumulations are taken as often as you wanted? What if media errors occur? Identifying these types of conditions is critical to ensuring a successful recovery.

Automated Recovery

Having people with the required expertise to perform recoveries is a major consideration, particularly in disaster situations. For example, if the only person who understands your IBM Information Management System (IMS) systems (hierarchical database system) and can recover them moved far away, you're in trouble. However, if your recovery processes are planned and automated so that less-experienced personnel can aid in or manage the recovery process, then you're able to maximize all your resources and reduce the risk to your business.

Automation takes some of the human error factor and "think time" out of the recovery equation and makes the complexity of the environment less of a concern. Creating an automated and easy-to-use system requires the right tools and some planning for the inevitable, but compared to the possible loss of the entire business, it is worth the investment. With proper planning and automation, recovery is made possible, reliance on specific personnel is reduced, and the human-error factor is nearly eliminated.

Creating the recovery job control language (JCL) for your IMS systems is not as simple as modifying existing JCL to change the appropriate names. In the event of a disaster, the IMS recovery control (RECON) data sets must be modified in preparation for the recovery. RECON backups are usually taken while IMS is up, which leaves the RECONs in need of many clean-up activities before they can be used to perform a recovery: deleting online log data sets (OLDS), closing logistics supportability (LOGS), deleting subsystems (SUBSYS) records, and so on. This process often takes hours to perform manually, with the system down, equating to lost money. Planning for RECON clean-up is an important but often-overlooked step of the preparation process; discovering a deficiency in this area at disaster-recovery time is too late.

Make Recoveries Efficient

Planning for efficient recoveries is also critical. Multithreading tasks shorten the recovery process. Recovering multiple databases with one pass through your log data certainly will save time. Taking image copies, rebuilding indexes, and validating pointers concurrently with the recovery process further reduce downtime. Where downtime is costly, time saved is money in the bank. Any measures you can take to perform recovery and related tasks more quickly and efficiently allow your business to resume faster and save money.

Take Backups

After you've thought about and planned for your recoveries, it's time to think about executing your plan. Clearly the first step to a successful recovery is the backup of your data. Your goal in backing up data is to do so quickly, efficiently, and usually with minimal impact to your customers. If you have a large window where systems aren't available, standard image copies are your best option. These clean copies are good recovery points and are easy to manage. If, however, you need to take backups while systems are active, you may need some help. You can take advantage of recent technological changes in various ways. You might need only very brief outages to take instant copies of your data, or you might have intelligent storage devices that allow you to take a snapshot of your data. Both methods call for tools to assist in the management of resources.

HIDING AND RECOVERING HIDDEN DATA

It is common knowledge that what is deleted from the computer can sometimes be brought back. Recent analysis of security implications of "alternative datastreams" on Windows NT has shown that Windows NTFS filesystem allows data hiding in alternative datastreams connected to files. These datastreams are not destroyed by many file wiping utilities that promise irrecoverable removal of information. Wiping the file means "securely" deleting it from disk (unlike the usual removal of file entries from directories), so that file restoration becomes extremely expensive or impossible [5].

For example, Linux has no alternative data streams, but files removed using `/bin/rm` still remain on the disk. Most Linux systems use the ext2 filesystem (or its journaling version, ext3 by Red Hat). A casual look at the design of the ext2 filesystem shows several places where data can be hidden [5].

Let's start with the classic method to hide material on UNIX filesystems (not even ext2 specific). Run a process that keeps the file open and then remove the file. The file contents are still on disk and the space will not be reclaimed by other programs [5].

If an executable erases itself, its contents can be retrieved from /proc memory image: command "cp /proc/$PID/exe /tmp/file" creates a copy of a file in /tmp.

If the file is removed by `/bin/rm`, its content still remains on disk, unless overwritten by other files. Several Linux unerase utilities including `e2undel` attempt automated recovery of files. They are based on Linux Ext2fs Undeletion mini-HOWTO that provides a nice guide to file recovery from Linux partitions. Recovery can also be performed manually using debugfs Linux utility (as described in the preceding HOWTO) [5].

Overall, if recovery is attempted shortly after file removal and the partition is promptly unmounted, chances of complete recovery are high. If the system was heavily used, the probability of successful data undeletion significantly decreases. However, if you are to look at the problem from the forensics point of view, the chances of recovering something (such as a small part of the illegal image for the prosecution) is still very high. It was reported that sometimes parts of files from several years ago are found by forensic examiners [5].

Thus, files can be hidden in free space. If many copies of the same file are saved and then erased, the chance of getting the contents back becomes higher using the preceding recovery methods. However, due to the intricacies of ext2 filesystem, the process can only be reliably automated for small files [5].

A more detailed look at ext2 internals reveals the existence of slack space. Filesystem uses addressable parts of disks called blocks, which have the same size. Ext2 filesystems typically use 1-, 2-, or 4-KB blocks. If a file is smaller than the block size, the remaining space is wasted. It is called slack space. This problem long plagued early Windows 9x users with FAT16 filesystems, which had to use block sizes of up to 32 K, thus wasting a huge amount of space if storing small files [5].

On a 4-gigabyte Linux partition, the block size is typically 4 K (chosen automatically when the mke2fs utility is run to create a filesystem). Thus, one can reliably hide up to 4 KB of data per file if using a small file. The data will be invulnerable to disk usage, invisible from the filesystem, and, more exciting for some people, undetectable by file integrity checkers using file checksumming algorithms and MAC times. Ext2 floppy (with a block size of 1 KB) allows hiding data as well, albeit in smaller chunks [5].

The obscure tool bmap exists to jam data in slack space, take it out and also wipe the slack space, if needed. Some of the examples follow [5]:

```
# echo "evil data is here" | bmap —mode putslack /etc/passwd
```

puts the data in slack space produced by, `/etc/passwd file`

```
# bmap —mode slack /etc/passwd
getting from block 887048
file size was: 9428
slack size: 2860
block size: 4096
evil data is here
```

shows the data

```
# bmap —mode wipeslack /etc/passwd
```

cleans the slack space.

Data can be hidden in slack space to store secrets, plant evidence (forensics software will find it, but the suspect probably will not), and maybe hide tools from integrity checkers (if automated splitting of the larger file into slack-sized chunks is implemented). Now let's turn to discovering what is out there on the vast expanses of the disk drive. If looking for strings of text, a simple "`strings /dev/hdaX | grep 'string we need'`" will confirm the presence of string on the partition (the process will take a long time). Using a hex editor on the raw partition can sometimes shed some light on the disk contents, but the process is extremely messy. Thus, further analysis puts us firmly in the field of computer forensics [5].

Next, let's briefly review how to prevent adversaries from finding private data. Several Linux file cleansing utilities exist. All but one can only be used to wipe files, rather than empty disk space. Some use the multiple random passes and some simply overwrite the file with zeros once. Some do not work under certain circumstances or for specific filesystems. As reported in shred man page, "shred relies on a very important assumption: that the filesystem overwrites data in place." If this condition is not met, no secure deletion will be performed (with no error message) [5].

To eliminate the traces of old removed files, one might want to wipe the empty space. The simple method is to use a standard Linux “`dd`” utility. To wipe the empty space on the `/home` partition use

1. `dd if=/dev/zero of=/home/bigfile`
2. `sync`
3. `rm /home/bigfile`
4. `sync` [5]

The commands will zero out the empty space on the partition. Doing the same for the `/tmp` partition might cause some applications to crash, so one must be cautious [5].

NOTE *Swap space can also contain pieces of private data and should be wiped as well if additional security is desired.*

The important fact is that when empty space is wiped, slack space for all files remains intact. If a file is wiped (at least using the current version of GNU shred), the associated slack space is NOT wiped with it [5].

This section briefly touched upon hiding, finding, and destroying data on Linux filesystems. It should become clear that the area of computer forensics aimed at recovering the evidence from captured disk drives has many challenges, requiring knowledge of hardware, operating systems, and application software [5].

Finally, let’s look at some disk and tape data-recovery case studies. Additional case studies are found at the end of this chapter.

CASE HISTORIES

If there is any data, anywhere on your disk or tape, it can be recovered. Let’s take a look at some of the more interesting disk-recovery case studies.

A Dog’s Dinner

Late one afternoon, customer service received a phone call from a distraught customer who required data recovery from a couple of diskettes. The data was related to an important presentation. The customer was asked the nature of the problem and eventually confessed that the diskettes had suffered some *physical damage*. The problem involved one of his four-legged canine friends who had chewed the diskettes.

The damage to the disk cases was severe, with large tooth marks evident on the surface of the disks. Eventually both disks were imaged with only 15% sector damage, and the file allocation tables (FATs) were rebuilt. All the files were successfully recovered and restored to the grateful customer.

Credit Card Monster

The customer was a well-known credit card company whose last few hours' transactions, for which there was no backup, were stored on a failed system. This was a NetWare Server and RAID array in one large, very heavy metal box, containing 18 × 2.5–gigabyte wide SCSI drives and weighing nearly 200 kg.

There were three failed drives amongst the remaining batch of eight drives. One of the drives had suffered component failure on its electronics assembly; the other two had serious head/disk assembly (HDA) problems that needed work in a cleanroom. Using a database of drive components and technical knowledge, the system administrator worked to correct the faults on the drives so he could take images.

When he finally finished, all 18 drives had been imaged, with a total sector loss of just 7 bad sectors. The total good sectors imaged that night was just under 88 million! The customer's valuable data was safe.

Flying Low

Having flown numerous times on business without a problem, one customer was surprised to find that his Toshiba laptop wouldn't boot. On contact with the system administrator, he finally mentioned that it had traveled in the cargo hold of a plane. The system administrator had a nagging suspicion that it had probably not only been thrown around by the baggage handlers, but also bounced its way down the carousel.

Luckily for him, it had not been swipe-damaged by x-ray equipment at the airport. Hardware specialists opened the head disk assembly and found there was some speckle damage, confirming that it had been bounced around, as the heads had dented the actual platters. Following a successful headstack swap, the drive was imaged and the system administrator found 112 bad sectors, of which he was finally able to read only 86. The customer vowed always to take his laptop as carry-on luggage from then on.

Accounts Critical

It was Easter Saturday and the system administrator had a critical tape data loss that another data-recovery company had failed to rectify. Within about four hours of receiving the first tape, the system administrator had several hundred megabytes of data from it. The tape was poorly recorded and had many areas where the recording had broken up.

The customer had a set of about 35 tapes in this condition, which the system administrator also needed to look at. By 6 A.M. on Sunday, the system administrator was recovering data from seven DAT tapes and had extracted images of each of the disks in the RAID. A few hours later, most of the physical data had been recovered. The areas of missing data were being reprocessed to attempt to extract additional data from the tapes. However, the data of major importance was from the accounts system. About 48 hours later, the system administrator was still working on reading data from the damaged areas of the tapes. By the end of the following week, all the data had been successfully recovered—no mean feat considering the huge amount of data involved.

Sinking Ship

A seismic survey ship far away in a distant sea sent a system administrator an IBM 3590 tape. It contained the results of a number of geological surveys as part of a search for oil, but also contained a media flaw right at the start. If the data could not be recovered, they would have to send the ship back out to sea to repeat the tests—a rather costly operation.

At the time, the IBM 3590 drive was one of the fastest tape drives around. The 40 kg monster is capable of storing 10 gigabyte of uncompressed data on a single cartridge and transferring that data at up to 9 MB per second. At the heart of this mechanism is a read-write-head that records 16 data tracks at a time.

Gaining control of these various systems, finding the undamaged data on the tape, and then persuading the drive to read it was complex. However, after much perseverance, all the important data was safely on one of the systems, and the system administrator could call for a courier to take the data back to Singapore.

All Flooded Out

A business continuity firm had a customer with a big problem. A firm of automotive engineers had archived their important drawings and documents in a locked fireproof safe in their basement. Sadly, a flood had filled the basement with water and fine silt, and the engineers found that their archives and backups were soaked through and the media was coated inside and out with a thin layer of sediment.

In total, over 40 tape and optical cartridges of various formats had been affected, and some of the tapes had started to dry while still in the safe. Each tape was extracted from its cartridge and installed in a special cleaning rig that removed any sediment. Once clean, the tape was then placed in a brand new cartridge assembly so that the data could be read. After a few hours, the system administrator was able to return the recovered files and folders on a total of 26 CD-ROMs; the engineers were grateful for the return of their archives.

A Concluding Case Study Example

As an almost real-life example, XYZ Corporation is an IMS shop with headquarters in Houston, Texas. Tropical Storm Allison visits the Texas Gulf coast and dumps three feet of rain on the city. XYZ, with its state-of-the-art data center located in the heart of the city, takes on a basement full of water. Their uninterruptible power supply (UPS) system, network switches, and a portion of their direct access storage devices (DASDs) are wiped out.

Preparations

Being good corporate citizens and experienced users of the biennial reporting system (BRS), XYZ is in great condition to recover. They take weekly image copies, creating dual copies concurrently so the second copy can be sent off-site. They run nightly change accumulations to consolidate their updates and send secondary certification authorities (CAs) off-site each morning at 6 A.M. Copies of logs are dispatched to off-site storage at 6 P.M. Recovery Advisor jobs are scheduled to make sure that image copies and change accumulations are performed at the specified intervals. They run the Check Assets function regularly to ensure that required assets are cataloged. Regular disaster-recovery drills let them practice, so their people know what to do.

Proof

Finally, when disaster strikes, XYZ springs into action, and the validity of their preparations is proved. They call their local disaster-recovery (DR) service provider, arrange for shipment of their tapes, and rush to the hot site. They initial program load (IPL) their system and bring up the Recovery Manager interface. They use the RECON cleanup utility to prepare the IMS RECONs for restart. They build the appropriate groups for their lost databases and build appropriate recovery JCL. The recovery utility runs, calling in the appropriate image copy, change accumulation, and log data. Their data is restored without errors, their business resumes quickly, and everyone lives happily ever after, all with minimal expense and elapsed time.

SUMMARY

With ever-larger information sets being kept on-line, how quickly can data be restored and brought back into production? It is in addressing this requirement that the demand has arisen for new and more sophisticated data management and data-recovery techniques.

Backup has never really been the problem. A variety of backup tools (both hardware and software) have been available for a number of years. Although data backups would seem to offer an effective shield against these threats, backups do not always provide comprehensive data protection. That is because the data backup plans developed by many companies are not fully realized or, worse yet, not followed. What is more, individuals often fail to test the restore capabilities of their backup media. If the backups are faulty, a simple data loss can quickly become a data disaster. Finally, even if backups are successful, they only contain data collected during the most recent backup session. As a result, a data loss can potentially rob you of your most current data, despite your backup attempts.

Conclusions

- Data backup and recovery has become the "killer application" of storage area networking.
- The ability to move data directly from disk to tape at 400 MB/second will offer performance levels that are unprecedented by today's standards.
- SAN-based backup offers benefits such as higher availability, increased flexibility, improved reliability, lower cost, manageability, improved performance, and increased scalability.
- IT professionals face a number of challenges in today's marketplace. Whether your business is retail, health care, banking, manufacturing, public utility, government agency, or almost any other endeavor, one thing is common: your users expect more and more from your systems.
- Computer systems have grown to manage much of the business world. How does this growth affect your daily management of the data? What challenges do you face? If a problem occurs, how do you get your applications back to normal in the most efficient manner possible?
- Some files (especially on Linux systems) can and should be recovered with very little effort or time. While it can take a great deal of time to actually recover something, wizardly skill is not really required.
- Ultimately, your odds of getting anything useful from the grave (dead storage) is often a question of personal diligence—how much is it worth to you? If it's important enough, it's quite possibly there.
- The persistence of data, however, is remarkable. Contrary to the popular belief that it's hard to recover information, it's actually starting to appear that it's very hard to remove something even if you want to.
- Indeed, when testing forensic software on a disk that had been used for some time on a Windows 2000, XP or 2003 machine, then reinstalled to be a firewall using Solaris, and finally converted to be a Linux system, files and data from the prior two installations are clearly visible. Now that's data persistence.

- Forensic data is everywhere on computers. You need to continue the examination, for you have simply scratched the surface.

An Agenda for Action

When completing the Data Recovery Checklist (Table F5.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for data recovery. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Data recovery is the process by which mediocre trained engineers evaluate and extract data from damaged media and return it in an intact format.
2. True or False? Fortunately, there are very few specialized hardware and software companies that manufacture products for the centralized backup and recovery of business-critical data.
3. True or False? Operationally, ready, or mirrored data does guard against data corruption and user error.
4. True or False? One of the most critical data-management tasks involves recovering data in the event of a solution.
5. True or False? Wiping the file means "securely" adding it from disk (unlike the usual removal of file entries from directories), so that file restoration becomes extremely expensive or impossible.

Multiple Choice

1. The following are obstacles to backing up applications, except:

   A. Backup window
   B. Network bandwidth
   C. Wireless bandwidth

D. System throughput
E. Lack of resources

2. There are three I/O bottlenecks commonly found in traditional backup schemes, except for two:

A. The ability of the system being backed up to push data to the backup server
B. The ability of the backup server to not accept data from multiple systems simultaneously
C. The ability of the backup server to accept data from multiple systems simultaneously
D. The available throughput of the tape device(s) onto which the data is moved
E. The available throughput of the tape device(s) onto which the data is stable

3. Below, are three of many factors that affect backup, except:

A. Storage costs are increasing.
B. Systems have to be online continuously.
C. The role of backup has changed.
D. Storage costs are decreasing.
E. The role of backup has not changed.

4. Successful data backup and recovery is composed of four key elements, except:

A. The backup server
B. The hardware
C. The network
D. The backup window
E. The backup storage device (or devices)

5. Unfortunately, many companies are already struggling with simply managing the existing data traffic created by applications such as the following, except one:

A. E-commerce
B. Internet
C. Email
D. Snail mail
E. Multimedia document management.

Exercise

A local lumber company went up in flames in late September. The fire safe where they kept their backups had been left open that night after closing. How would the CFS handle this problem?

HANDS-ON PROJECTS

After being sued for negligence, a corporation was about to settle a multimillion dollar suit and rewrite their entire software package because the plaintiff was charging that installation of the software in question had permanently damaged or erased existing files, the irreplaceable data was not recoverable by any means, and he could not access files in a specific software application critical to running his business. How would the firm's CFS team (CFST) go about investigating this case?

Case Project

Five fire-damaged UNIX server drives were literally shoveled out of the debris from a large auto dealership fire. The (plastic-material) backup tapes had been co-located with the server drives and were themselves destroyed. All financial data (inventory, accounts payable and receivable, W-2s, customers and loan information) was destroyed. How would a CFST go about investigating this incident?

Optional Team Case Project

In a breach of contract case, it was decided on a Friday to use the CFST to recover company emails. The attorney immediately needed all of the plaintiff company's emails and attachments over a six-month time frame meeting keyword and time and date criteria. Over 1,091,000 emails met the criteria. Emails and the system were password protected and the passwords were not available. Explain the CFST's solution in detail regarding the organization's investigation into this matter.

REFERENCES

[1] Gamradt, Derek, "Data Backup + Recovery," StorNet, Corporate Headquarters, 7074 South Revere Parkway, Englewood, CO 80112, 2001.

[2] Vacca, John R., *Electronic Commerce: Online Ordering and Digital Money,* Charles River Media, Hingham, MA, 2001.

[3] StorNet, Corporate Headquarters, 7074 South Revere Parkway, Englewood, CO 80112, 2001.

[4] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

[5] Chuvakin, Anton, "Linux Data Hiding and Recovery" (© 2000–2004 Anton Chuvakin), Edison, NJ/Long Island, NY.

6 Evidence Collection and Data Seizure

Evidence is difficult to collect at the best of times, but when that evidence is electronic, an investigator faces some extra complexities. Electronic evidence has none of the permanence that conventional evidence has, and it is even more difficult to form into a coherent argument. The purpose of this chapter is to point out these difficulties and describe what must be done to overcome them. Not everything is covered here. It should be used as a guide only, and you should seek further information for your specific circumstances.

NOTE

No legal advice is given here—different regions have different legislation. If in doubt, always ask your lawyer—that's what they're there for.

This part of the chapter is not aimed at expert forensics analysts, as most of this would be obvious to them. Nor is it to be seen as the correct answer to all investigations on a computer system. The simple reason for this is that there never is one correct answer that will guide you through all investigations. No two investigations are the same, and the only thing you can ever be sure about when arriving at the scene is that there is nothing you can be sure about.

WHY COLLECT EVIDENCE?

Electronic evidence can be very expensive to collect. The processes are strict and exhaustive, the systems affected may be unavailable for regular use for a long period of time, and analysis of the data collected must be performed. So, why bother collecting the evidence in the first place? There are two simple reasons: future prevention and responsibility.

Future Prevention

Without knowing what happened, you have no hope of ever being able to stop someone else (or even the original attacker) from doing it again. It would be analogous to not fixing the lock on your door after someone broke in. Even though the cost of collection can be high, the cost of repeatedly recovering from compromises is much higher, both in monetary and corporate image terms.

Responsibility

There are two responsible parties after an attack: the attacker and the victim. The attacker is responsible for the damage done, and the only way to bring him to justice (and to seek recompense) is with adequate evidence to prove his actions.

The victim, on the other hand, has a responsibility to the community. Information gathered after a compromise can be examined and used by others to prevent further attacks. The victim may also have a legal obligation to perform an analysis of evidence collected, for instance if the attack on their system was part of a larger attack.

COLLECTION OPTIONS

Once a compromise has been detected, you have two options: pull the system off the network and begin collecting evidence or leave it online and attempt to monitor the intruder. Both have their pros and cons. In the case of monitoring, you may accidentally alert the intruder while monitoring and cause him to wipe his tracks any way necessary, destroying evidence as he goes. You also leave yourself open to possible liability issues if the attacker launches further attacks at other systems from your own network system. If you disconnect the system from the network, you may find that you have insufficient evidence or, worse, that the attacker left a *dead man switch* that destroys any evidence once the system detects that it's offline. What you choose to do should be based on the situation. The "Collection and Archiving" section later in the chapter contains information on what to do for either case.

OBSTACLES

Electronic crime is difficult to investigate and prosecute. Investigators have to build their case purely on any records left after the transactions have been completed.

Add to this the fact that electronic records are extremely (and sometimes transparently) malleable and that electronic transactions currently have fewer limitations than their paper-based counterparts and you get a collection nightmare.

Computer transactions are fast, they can be conducted from anywhere (through anywhere, to anywhere), can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible. Any *paper trail* of computer records they may leave can be easily modified or destroyed, or may be only temporary. Worse still, auditing programs may automatically destroy the records left when computer transactions are finished with them.

Because of this, even if the details of the transactions can be restored through analysis, it is very difficult to tie the transaction to a person. *Identifying* information such as passwords or PIN numbers (or any other electronic identifier) does not prove who was responsible for the transaction. Such information merely shows that whoever did it either knew or could get past those identifiers.

Even though technology is constantly evolving, investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously. The best you can do is to follow the rules of evidence collection and be as assiduous as possible.

TYPES OF EVIDENCE

Before you start collecting evidence, it is important to know the different types of evidence categories. Without taking these into consideration, you may find that the evidence you've spent several weeks and quite a bit of money collecting is useless. Real evidence is any evidence that speaks for itself without relying on anything else. In electronic terms, this can be a log produced by an audit function—provided that the log can be shown to be free from contamination.

Testimonial Evidence

Testimonial evidence is any evidence supplied by a witness. This type of evidence is subject to the perceived reliability of the witness, but as long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence. Word processor documents written by a witness may be considered testimonial—as long as the author is willing to state that he wrote it.

Hearsay

Hearsay is any evidence presented by a person who was not a direct witness. Word processor documents written by someone without direct knowledge of the incident are hearsay. Hearsay is generally inadmissible in court and should be avoided.

THE RULES OF EVIDENCE

There are five rules of collecting electronic evidence. These relate to five properties that evidence must have to be useful.

1. Admissible
2. Authentic
3. Complete
4. Reliable
5. Believable

Admissible

Admissible is the most basic rule. The evidence must be able to be used in court or otherwise. Failure to comply with this rule is equivalent to not collecting the evidence in the first place, except the cost is higher.

Authentic

If you can't tie the evidence positively to the incident, you can't use it to prove anything. You must be able to show that the evidence relates to the incident in a relevant way.

Complete

It's not enough to collect evidence that just shows one perspective of the incident. You collect not only evidence that can prove the attacker's actions, but also evidence that could prove their innocence. For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in and why you think they didn't do it. This is called *exculpatory evidence* and is an important part of proving a case.

Reliable

The evidence you collect must be reliable. Your evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.

Believable

The evidence you present should be clearly understandable and believable to a jury. There's no point presenting a binary dump of process memory if the jury has no idea what it all means. Similarly, if you present them with a formatted, human-understandable version, you must be able to show the relationship to the original binary, otherwise there's no way for the jury to know whether you've faked it. Using the preceding five rules, you can derive some basic do's and don'ts:

- Minimize handling and corruption of original data.
- Account for any changes and keep detailed logs of your actions.
- Comply with the five rules of evidence.
- Do not exceed your knowledge.
- Follow your local security policy.
- Capture as accurate an image of the system as possible.
- Be prepared to testify.
- Work fast.
- Proceed from volatile to persistent evidence.
- Don't shutdown before collecting evidence.
- Don't run any programs on the affected system.

Minimize Handling and Corruption of Original Data

Once you've created a master copy of the original data, don't touch it or the original. Always handle secondary copies. Any changes made to the originals will affect the outcomes of any analysis later done to copies. You should make sure you don't run any programs that modify the access times of all files (such as tar and xcopy). You should also remove any external avenues for change and, in general, analyze the evidence after it has been collected.

Account for Any Changes and Keep Detailed Logs of Your Actions

Sometimes evidence alteration is unavoidable. In these cases, it is absolutely essential that the nature, extent, and reasons for the changes be documented. Any changes at all should be accounted for—not only data alteration but also physical alteration of the originals (the removal of hardware components).

Comply with the Five Rules of Evidence

The five rules are there for a reason. If you don't follow them, you are probably wasting your time and money. Following these rules is essential to guaranteeing successful evidence collection.

Do Not Exceed Your Knowledge

If you don't understand what you are doing, you can't account for any changes you make and you can't describe what exactly you did. If you ever find yourself "out of your depth," either go and learn more before continuing (if time is available) or find someone who knows the territory. Never soldier on regardless. You'll just damage your case.

Follow Your Local Security Policy

If you fail to comply with your company's security policy, you may find yourself with some difficulties. Not only may you end up in trouble (and possibly fired if you've done something really against policy), but you may not be able to use the evidence you've gathered. If in doubt, talk to those who know.

Capture as Accurate an Image of the System as Possible

Capturing an accurate image of the system is related to minimizing the handling or corruption of original data. Differences between the original system and the master copy count as a change to the data. You must be able to account for the differences.

Be Prepared to Testify

If you're not willing to testify to the evidence you have collected, you might as well stop before you start. Without the collector of the evidence being there to validate the documents created during the evidence-collection process, the evidence becomes hearsay, which is inadmissible. Remember that you may need to testify at a later time. No one is going to believe you if they can't replicate your actions and reach the same results. This also means that your plan of action shouldn't be based on trial-and-error.

Work Fast

The faster you work, the less likely the data is going to change. Volatile evidence may vanish entirely if you don't collect it in time. This is not to say that you should rush. You must still collect accurate data. If multiple systems are involved, work on them in parallel (a team of investigators would be handy here), but each single system should still be worked on methodically. Automation of certain tasks makes collection proceed even faster.

Proceed from Volatile to Persistent Evidence

Some electronic evidence (discussed later) is more volatile than others are. Because of this, you should always try to collect the most volatile evidence first.

Don't Shutdown Before Collecting Evidence

You should never, ever shutdown a system before you collect the evidence. Not only do you lose any volatile evidence, but also the attacker may have trojaned (via a trojan horse) the startup and shutdown scripts, plug-and-play devices may alter the system configuration, and temporary file systems may be wiped out. Rebooting is even worse and should be avoided at all costs. As a general rule, until the compromised disk is finished with and restored, it should never be used as a boot disk.

Don't Run Any Programs on the Affected System

Because the attacker may have left trojaned programs and libraries on the system, you may inadvertently trigger something that could change or destroy the evidence you're looking for. Any programs you use should be on read-only media (such as a CD-ROM or a write-protected floppy disk) and should be statically linked.

VOLATILE EVIDENCE

Not all the evidence on a system is going to last very long. Some evidence resides in storage that requires a consistent power supply; other evidence may be stored in information that is continuously changing [1]. When collecting evidence, you should always try to proceed from the most volatile to the least. Of course, you should still take the individual circumstances into account. You shouldn't waste time extracting information from an unimportant or unaffected machine's main memory when an important or affected machine's secondary memory hasn't been examined.

To determine what evidence to collect first, you should draw up an order of volatility—a list of evidence sources ordered by relative volatility. An example an order of volatility would be:

1. Registers and cache
2. Routing tables
3. Arp cache
4. Process table
5. Kernel statistics and modules
6. Main memory
7. Temporary file systems
8. Secondary memory
9. Router configuration
10. Network topology [2]

NOTE

Once you have collected the raw data from volatile sources you may be able to shut down the system.

GENERAL PROCEDURE

When collecting and analyzing evidence, there is a general four-step procedure you should follow. Note that this is a very general outline. You should customize the details to suit your situation.

Identification of Evidence

You must be able to distinguish between evidence and junk data. For this purpose, you should know what the data is, where it is located, and how it is stored. Once this is done, you will be able to work out the best way to retrieve and store any evidence you find.

Preservation of Evidence

The evidence you find must be preserved as close as possible to its original state. Any changes made during this phase must be documented and justified.

Analysis of Evidence

The stored evidence must then be analyzed to extract the relevant information and recreate the chain of events. Analysis requires in-depth knowledge of what you are looking for and how to get it. Always be sure that the person or people who are analyzing the evidence are fully qualified to do so.

Presentation of Evidence

Communicating the meaning of your evidence is vitally important—otherwise you can't do anything with it. The manner of presentation is important, and it must be understandable by a layman to be effective. It should remain technically correct and credible. A good presenter can help in this respect.

COLLECTING AND ARCHIVING

Once you've developed a plan of attack and identified the evidence that needs to be collected, it's time to start the actual process of capturing the data. Storage of that data is also important, as it can affect how the data is perceived.

Logs and Logging

You should run some kind of system logging function. It is important to keep these logs secure and to back them up periodically. Because logs are usually automatically timestamped, a simple copy should suffice, although you should digitally sign and encrypt any logs that are important to protect them from contamination. Remember, if the logs are kept locally on the compromised machine, they are susceptible to either alteration or deletion by an attacker. Having a remote syslog server and storing logs in a *sticky* directory can reduce this risk, although it is still possible for an attacker to add decoy or junk entries into the logs.

Regular auditing and accounting of your system is useful not only for detecting intruders but also as a form of evidence. Messages and logs from programs can be used to show what damage an attacker did. Of course, you need a clean snapshot for these to work, so there's no use trying it after the compromise.

Monitoring

Monitoring network traffic can be useful for many reasons—you can gather statistics, watch out for irregular activity (and possibly stop an intrusion before it happens), and trace where an attacker is coming from and what he is doing. Monitoring logs as they are created can often show you important information you might have missed had you seen them separately. This doesn't mean you should ignore logs later—it may be what's missing from the logs that is suspicious.

Information gathered while monitoring network traffic can be compiled into statistics to define normal behavior for your system. These statistics can be used as an early warning of an attacker's actions. You can also monitor the actions of your users. This can, once again, act as an early warning system. Unusual activity or the sudden appearance of unknown users should be considered definite cause for closer inspection.

No matter the type of monitoring done, you should be very careful. There are plenty of laws you could inadvertently break. In general, you should limit your monitoring to traffic or user information and leave the content unmonitored unless the situation necessitates it. You should also display a disclaimer stating what monitoring is done when users log on. The content of this should be worked out in conjunction with your lawyer.

METHODS OF COLLECTION

There are two basic forms of collection: *freezing the scene* and *honeypotting*. The two aren't mutually exclusive. You can collect *frozen* information after or during any honeypotting.

Freezing the scene involves taking a snapshot of the system in its compromised state. The necessary authorities should be notified (the police and your incident response and legal teams), but you shouldn't go out and tell the world just yet. You should then start to collect whatever data is important onto removable nonvolatile media in a standard format. Make sure the programs and utilities used to collect the data are also collected onto the same media as the data. All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification.

Honeypotting is the process of creating a replica system and luring the attacker into it for further monitoring. A related method (sandboxing) involves limiting what the attacker can do while still on the compromised system, so he can be monitored without (much) further damage. The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives. You must make sure that any data on the system related to the attacker's detection and actions is either removed or encrypted; otherwise they can cover their tracks by destroying it. Honeypotting and sandboxing are extremely resource intensive, so they may be infeasible to perform. There are also some legal issues to contend with, most importantly entrapment. As previously mentioned, you should consult your lawyers.

ARTIFACTS

Whenever a system is compromised, there is almost always something left behind by the attacker—be it code fragments, trojaned programs, running processes, or sniffer log files. These are known as *artifacts*. They are one of the important things you should collect, but you must be careful. You should never attempt to analyze an artifact on the compromised system. Artifacts are capable of anything, and you want to make sure their effects are controlled.

Artifacts may be difficult to find; trojaned programs may be identical in all obvious ways to the originals (file size, medium access control [MAC] times, etc.). Use of cryptographic checksums may be necessary, so you may need to know the original file's checksum. If you are performing regular file integrity assessments, this shouldn't be a problem. Analysis of artifacts can be useful in finding other systems the attacker (or his tools) has broken into.

COLLECTION STEPS

You now have enough information to build a step-by-step guide for the collection of the evidence. Once again, this is only a guide. You should customize it to your specific situation. You should perform the following collection steps:

1. Find the evidence.
2. Find the relevant data.

3. Create an order of volatility.
4. Remove external avenues of change.
5. Collect the evidence.
6. Document everything.

Find the Evidence

Determine where the evidence you are looking for is stored. Use a checklist. Not only does it help you to collect evidence, but it also can be used to double-check that everything you are looking for is there.

Find the Relevant Data

Once you've found the evidence, you must figure out what part of it is relevant to the case. In general, you should err on the side of over-collection, but you must remember that you have to work fast. Don't spend hours collecting information that is obviously useless.

Create an Order of Volatility

Now that you know exactly what to gather, work out the best order in which to gather it. The order of volatility for your system is a good guide and ensures that you minimize loss of uncorrupted evidence.

Remove External Avenues of Change

It is essential that you avoid alterations to the original data, and prevention is always better than a cure. Preventing anyone from tampering with the evidence helps you create as exact an image as possible. However, you have to be careful. The attacker may have been smart and left a dead-man switch. In the end, you should try to do as much as possible to prevent changes.

Collect the Evidence

You can now start to collect the evidence using the appropriate tools for the job. As you go, reevaluate the evidence you've already collected. You may find that you missed something important. Now is the time to make sure you get it.

Document Everything

Your collection procedures may be questioned later, so it is important that you document everything you do. Timestamps, digital signatures, and signed statements are all important. Don't leave anything out.

CONTROLLING CONTAMINATION: THE CHAIN OF CUSTODY

Once the data has been collected, it must be protected from contamination. Originals should never be used in forensic examination; verified duplicates should be used. This not only ensures that the original data remains clean, but also enables examiners to try more *dangerous*, potentially data-corrupting tests. Of course, any tests done should be done on a clean, isolated host machine. You don't want to make the problem worse by letting the attacker's programs get access to a network.

A good way of ensuring that data remains uncorrupted is to keep a chain of custody. This is a detailed list of what was done with the original copies once they were collected. Remember that this will be questioned later on, so document everything (who found the data, when and where it was transported [and how], who had access to it, and what they did with it). You may find that your documentation ends up greater than the data you collected, but it is necessary to prove your case.

Analysis

Once the data has been successfully collected, it must be analyzed to extract the evidence you wish to present and to rebuild what actually happened. As always, you must make sure that you fully document everything you do. Your work will be questioned and you must be able to show that your results are consistently obtainable from the procedures you performed.

Time

To reconstruct the events that led to your system being corrupted, you must be able to create a timeline. This can be particularly difficult when it comes to computers. Clock drift, delayed reporting, and differing time zones can create confusion in abundance. One thing to remember is to never, ever change the clock on an affected system. Record any clock drift and the time zone in use, as you will need this later, but changing the clock just adds in an extra level of complexity that is best avoided.

Log files usually use timestamps to indicate when an entry was added, and these must be synchronized to make sense. You should also use timestamps. You're not just reconstructing events, you yourself are making a chain of events that must be accounted for as well. It's best to use the GMT time zone when creating your timestamps. The incident may involve other time zones than your own, so using a common reference point can make things much easier.

Forensic Analysis of Backups

When analyzing backups, it is best to have a dedicated host for the job. This examination host should be secure, clean (a fresh, hardened install of the operating system is a good idea), and isolated from any network. You don't want it tampered with while you work, and you don't want to accidentally send something nasty down the line.

Once this system is available, you can commence analysis of the backups. Making mistakes at this point shouldn't be a problem. You can simply restore the backups again if required. Remember the mantra: Document everything you do. Ensure that what you do is repeatable and capable of always giving the same results.

RECONSTRUCTING THE ATTACK

Now that you have collected the data, you can attempt to reconstruct the chain of events leading to and following the attacker's break-in. You must correlate all the evidence you have gathered (which is why accurate timestamps are critical), so it's probably best to use graphical tools, diagrams, and spreadsheets. Include all of the evidence you've found when reconstructing the attack—no matter how small it is. You may miss something if you leave a piece of evidence out.

Finally, as you can see, collecting electronic evidence is no trivial matter. There are many complexities you must consider, and you must always be able to justify your actions. It is far from impossible though. The right tools and knowledge of how everything works is all you need to gather the evidence required.

SUMMARY

Companies spend millions each year to ensure that their networks and data are properly protected against intrusion. Operating systems are hardened, firewalls are installed, intrusion detection systems are put in place, honeypots are implemented, security policies and procedures are established, security awareness programs are rolled out, and systems are monitored. This defense-in-depth approach is used because companies know that people will try to gain unauthorized access to their systems. When unauthorized access does occur, the last line of defense is legal action against the intruder. However, if evidence of an intrusion is not properly handled, it becomes inadmissible in a court of law. It is important to remember one of the basic rules of our legal system: if there is no evidence of a crime, there is no crime in the eyes of the law. Therefore, it is of paramount importance that utmost care is taken in the collection and seizure of data evidence.

Some of the most common reasons for improper evidence collection are poorly written policies, lack of an established incident response plan, lack of incident response training, and a broken chain of custody. For the purposes of this chapter, the reader should assume that policies have been clearly defined and reviewed by legal counsel, an incident response plan is in place, and necessary personnel have been properly trained.

Conclusions

- Admissible is the most basic rule (the evidence must be able to be used in court or otherwise).
- If you can't tie the evidence positively with the incident, you can't use it to prove anything.
- It's not enough to collect evidence that just shows one perspective of the incident. You collect not only evidence that can prove the attacker's actions, but also evidence that could prove his innocence.
- Your evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.
- The evidence you present should be clearly understandable and believable by a jury.
- There are six fundamental rules to guide an investigator during a search and seizure. In essence, these rules are devised to help prevent the mishandling of evidence and encourage the documentation of search and seizure activities. In other words, the rules help ensure an investigation's chain of custody, which is critical to the success of any case.
- The preparation and team-structuring activities that take place help ensure a successful investigation. Without these activities, the chain of custody is put at great risk.
- The next three stages of the search and seizure process are approach and secure the crime scene, document the crime scene, and search for evidence.
- Crime scene security may range from locking doors to (for law enforcers) arresting trespassers.
- Documentation can be rough, but must be adequate in its depiction of the crime scene layout and the location of evidence.
- The search for evidence can involve looking in a variety of places, but the legalities of searching must always be considered.
- The virus protocol is a means of preventing and containing the threat to electronic evidence by computer viruses.

An Agenda for Action

When completing the Evidence Collection and Data Seizure Checklist (Table F6.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for evidence collection and data seizure. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? No two investigations you encounter will be the same.
2. True or False? Windows will not save a user's file search history, history of the last visited Internet sites, information filled out in Web forms, or the last programs used.
3. True or False? Bash history is not saved to file until an orderly shutdown is performed.
4. True or False? Electronic evidence is not very expensive to collect. The processes are strict and exhaustive, the systems affected may be unavailable for regular use for a long period of time, and analysis of the data collected must be performed.
5. True or False? Once a compromise has been detected, you have two options: pull the system off the network and begin collecting evidence or leave it offline and attempt to monitor the intruder.

Multiple Choice

1. Make sure you always document the following points, except::

   A. Who collected the evidence, how they did it and where they got it
   B. Who took possession of it
   C. How it was stored and protected
   D. How it was stored and unprotected
   E. Who removed it from storage and why

2. Make sure you always label any hardware with the following, except:

   A. A part number
   B. A case number

C. A short description of the hardware
D. The time and date you got the evidence
E. Your signature

3. There are five rules of collecting electronic evidence. These relate to the following five properties that evidence must have to be useful, except:

   A. Unadmissible
   B. Authentic
   C. Complete
   D. Reliable
   E. Believable

4. Using the five rules in multiple choice question 3, you can derive some basic do's and don'ts, except:

   A. Minimize handling/corruption of original data
   B. Account for any changes and keep detailed logs of your actions
   C. Comply with the six rules of evidence
   D. Do not exceed your knowledge
   E. Follow your local security policy

5. To determine what evidence to collect first, you should draw up an order of volatility—a list of evidence sources ordered by relative volatility. An example of an order of volatility would be the following, except:

   A. Registers and cache
   B. Routing tables
   C. Arp cache
   D. Process table
   E. Table statistics and modules

Exercise

A computer forensics specialist was called on a teenage runaway case. Why would a CFS be called in to solve a teenage runaway case? What would his role be here?

HANDS-ON PROJECTS

A parent was concerned that her son was accessing pornographic Web sites from his computer. Each time the computer was checked by a technician, no evidence was found. How would a CFS go about investigating this incident?

Case Project

An adult roommate was accused of using another's computer to make unauthorized purchases on a popular Internet shopping site. What did the CFS do after he conducted an investigation?

Optional Team Case Project

A female executive assistant was fired from a major U.S. chemical company. The former employee filed a lawsuit accusing her superiors at the company of sexual harassment and wrongful termination. Explain how a CFS would deal with this case.

REFERENCES

[1] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

[2] Braid, Matthew, "Collecting Electronic Evidence After a System Compromise," Australian Computer Emergency Response Team (AusCERT), The University of Queensland, Qld 4072 Australia (SANS Institute, 5401 Westbard Ave. Suite 1501, Bethesda, MD 20816), 2001.

This page intentionally left blank

7 Duplication and Preservation of Digital Evidence

Computer evidence is odd, to say the least. It lurks on computer hard disk drives, zip disks, and floppy diskettes at three different levels. Two of these levels are not visible to the computer user. Such evidence is fragile and can easily be destroyed by something as simple as the normal operation of the computer. Electromagnets and planted destructive trojan horse programs are other hazards that can permanently destroy computer evidence within seconds. There is no other type of evidence that presents the investigator with as many potential problems and challenges. In the old days, defense lawyers didn't know much about computer evidence. As a result, cross-examination by the defense wasn't as strong a few years ago as it is today. However, things are changing because lawyers are becoming educated because of the current popularity of electronic document discovery in the legal community. Times have changed and it is all the more important to do things by the book [1].

Nevertheless, computer forensic evidence is frequently challenged in court. Some judges accept it with little question because they want to crack down on computer criminals, and others reject it because they hold to a fairly technophobic view of the Fourth Amendment. There's also some confusion over the legal classification of computer evidence. Is it documentary evidence (which would require reams of printout under the best evidence rule) or is it demonstrative evidence (which would require a true-to-life sample of the reconstructed evidence)? Then there's the problem of establishing the expertise of cyber forensic experts who testify. The complexity of the criminal law means that the overwhelming majority of cases do not make it to civil or criminal court, but should [1].

The three criminal evidence rules to gain admissibility are

1. Authentication
2. The best evidence rule
3. Exceptions to the hearsay rule [1]

Authentication means showing a true copy of the original; best evidence means presenting the original; and the allowable exceptions are when a confession or business or official records are involved. Authentication appears to be the most commonly used rule, but experts disagree over what is the most essential, or most correct, element of this in practice. Some say documentation (of what has been done); others say preservation (the integrity of the original); still others say authenticity (the evidence being what you say it is). Good arguments could be made for the centrality of each, or all, as the standard in computer forensic law [1].

If your documentation is poor, it will look like your processing procedures were poor, and when you testify in court, you will look ridiculous since you have no good written record to refresh your memory. Problems in the documentation area arise when you try to take shortcuts or make do with less than adequate time, equipment, and resources. In general, the condition of all evidence has to be documented. It has to be photographed, weighed, and sketched, for example. Then, the laboratory worker (forensic scientist or criminalist) figures out what tests are appropriate, decides on what part of the evidence to examine first, dissects or copies the part to be tested (specimen = dissection; exemplar = copying), and prepares the testing ground, all the while documenting each decision step. Only then does any testing begin, and that's heavily documented with bench notes that are subject to discovery and review by experts from the other side [1].

If your preservation is poor, it becomes fairly evident that your collection and transportation of evidence gives rise to numerous possibilities for error in the form of destruction, mishandling, and contamination. Problems in the preservation area have implications for the integrity of law enforcement and crime labs. The basic chain of custody, for example, involves at least three initial sources of error. Evidence has to be discovered (police), it has to be collected (crime scene technician), and then it has to be packaged, labeled, and transported (police supervisor). Once it gets to the lab, it has to be logged in, assigned an identification number, placed in storage, and kept from intermingling with other evidence. All workplaces must be clean and contamination free. Some workplaces are required to meet the standards of professional accrediting organizations. Written policies have to be in place. The quality assurance policy, for example, must act as a check on quality control. Some employee job titles must be held by those with college degrees in the appropriate field [1].

If your authenticity is poor, then you, your agency, and the prosecutor will look like inexperienced rookies, not so much foolish, but like rank amateurs who can't explain, for example, how an “MD5 Hash algorithm” works. Computer evidence, like computer simulations, hasn’t fared all that well under the rigorous standards of admissibility for scientific evidence. The old common law standard is *oculis subjecta fidelibus*, as it is for any piece of demonstrative evidence (like a plaster cast model; if the scale is 1:10, an average person ought to be able to visualize the larger thing to scale). Case law, however, varies by jurisdiction. Only the Marx standard resembles the old common law standard, and it’s only found in a handful of jurisdictions. Here’s a list of all the scientific evidence standards [1]:

Relevancy test (FRE 401, 402, 403): This is embodied in the Federal Rules of Evidence and some state versions that liberally allow anything that materially assists the trier of fact to be deemed relevant by the trier of law.

Frye standard (Frye v. U.S., 1923): For the results of a scientific technique to be admissible, the technique must be sufficiently established to have gained general acceptance in its particular field. This is a “general acceptance” test.

Coppolino standard (Coppolino v. State, 1968): The court allows a novel test or piece of new, sometimes controversial, science on a particular problem at hand if an adequate foundation can be laid, even if the profession as a whole isn’t familiar with it.

Marx standard (People v. Marx, 1975): The court is satisfied that it did not have to sacrifice its common sense in understanding and evaluating the scientific expertise put before it. This is a “common sense” or “no scientific jargon” test.

Daubert standard (Daubert v. Merrell Dow, 1993): This rigorous test requires special pretrial hearings for scientific evidence and special procedures on discovery where the rules are laid out beforehand on validity, reliability, benchmarking, algorithms, and error rates [1].

The federal courts were the first to recognize that files on computers were similar, but unlike, files kept on paper. The best evidence rule has also, in recent years, seen the growth of a standard known as representational accuracy, which means you don’t have to present all the originals. Therefore, a modern clause exists in the Federal Rules of Evidence (FRE 1001-3) that states, If data are stored by computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original [1].

This exception to the best evidence rule has found a mostly welcome reception in state courts, and you should argue that it’s more appropriate to consider digital evidence as demonstrative than documentary. The history of computers in the courtroom ties in with demonstrative standards, and computer forensics, after all, is about reconstructing the crime, or criminalistics. You see how apparent this is once you realize that investigators and technicians always work from a copy, duplicate, mirror, replica, or exemplar of the original evidence. Digital evidence is the most easily lost evidence. There's nothing in criminal justice more easily damaged, corrupted, or erased. You need to be able to demonstrate that the evidence is what you say it is, came from where you say it did, and has not been modified in any way since you obtained it. How you go about that depends on the circumstances and the computer systems you're dealing with. It's futile to talk about any one correct way to do it, or any perfect printout. There's no "silver bullet" standardized checklist, and there's no "magic" software to produce the perfect printout [1].

Now let's look at some of the emerging principles of duplication and preservation of digital evidence collection and handling. Many regard this as the skillset of computer forensics.

PRESERVING THE DIGITAL CRIME SCENE

The computer investigator not only needs to be worried about destructive process and devices being planted by the computer owner, he or she also needs to be concerned about the operating system of the computer and applications. Evidence is easily found in typical storage areas (spreadsheet, database, and word processing files). Unfortunately potential evidence can also reside in file slack, erased files, and the Windows swap file. Such evidence is usually in the form of data fragments and can be easily overwritten by something as simple as the booting of the computer or the running of Microsoft Windows. When Windows starts, it potentially creates new files and opens existing ones as a normal process. This situation can cause erased files to be overwritten, and data previously stored in the Windows swap file can be altered or destroyed. Furthermore, all of the Windows operating systems (Windows 2000, XP and especially 2003) have a habit of updating directory entries for files as a normal operating process. As you can imagine, file dates are important from an evidence standpoint.

Another concern of the computer investigator is the running of any programs on the subject computer. Criminals can easily modify the operating system to destroy evidence when standard operating systems commands are executed. Perpetrators could modify the operating system such that the execution of the DIR command destroys simulated evidence. Standard program names and familiar Windows program icons can also be altered and tied to destructive processes by a crafty high-tech criminal.

Even trusted word processing programs such as Microsoft Word and WordPerfect™ can become the enemy of the cyber cop. It works this way: When word processing files are opened and viewed, the word processing program creates temporary files. These files overwrite the temporary files that existed previously, and potential evidence stored in those files can be lost forever. There's a point to all of this. Computer evidence processing is risky business and is fraught with potential problems. Of course, any loss of crucial evidence or exculpatory material falls on the shoulders of the computer investigator. What will your answer be if the defense attorney claims the data you destroyed proved the innocence of his or her client? You had better have a good answer.

Many inherent problems associated with computer evidence processing vanish when tried and proven processing procedures are followed. The objective of this section is to keep Murphy's law from ruining your case. When it comes to computer evidence processing, Murphy is always looking over your shoulder. He stands ready to strike at just the wrong moment.

Your first objective, after securing the computer, should be to make a complete bit stream backup of all computer data before it is reviewed or processed. This should normally be done before the computer is operated. Preservation of evidence is the primary element of all criminal investigations, and computer evidence is certainly no exception. These basic rules of evidence never change. Even rookies know that evidence must be preserved at all costs. As stated previously, evidence can reside at multiple levels and in bizarre storage locations. These levels include allocated files, file slack, and erased files. It is not enough to do a standard backup of a hard disk drive. To do so would eliminate the backup of file slack and erased file space. Without backing up evidence in these unique areas, the evidence is susceptible to damage and modification by the computer investigator. Bit stream backups are much more thorough than standard backups. They involve copying of every bit of data on a storage device, and it is recommended that two such copies be made of the original when hard disk drives are involved. Any processing should be performed on one of the backup copies. As previously recommended, the original evidence should be preserved at all costs. After all, it is the *best evidence.*

The importance of bit stream image backups cannot be stressed enough. To process a computer hard disk drive for evidence without a bit stream image backup is like playing with fire in a gas station. The basic rule is that only on rare occasions should you process computer evidence without first making an image backup. The hard disk drive should be imaged using a specialized bit stream backup product.

To avoid getting too technical for the purposes of this chapter, specifics regarding the uses of these backup programs will be avoided. However, instruction manuals should be studied thoroughly before you attempt to process computer evidence. Ideally, you should conduct tests on your own computers beforehand and compare the results with the original computer evidence. Being comfortable with the software you use is an important part of computer evidence processing. Know your tools. Practice using all of your forensic software tools before you use them for processing of computer evidence. You may only get one chance to do it right.

COMPUTER EVIDENCE PROCESSING STEPS

Computer evidence is fragile by its very nature, and the problem is compounded by the potential of destructive programs and hidden data. Even the normal operation of the computer can destroy computer evidence that might be lurking in unallocated space, file slack, or in the Windows swap file. There really are no strict rules that must be followed regarding the processing of computer evidence. Every case is different, and flexibility on the part of the computer investigator is important.

With that in mind, the following general computer evidence processing steps have been provided. Remember that these do not represent the only true way of processing computer evidence. They are general guidelines provided as food for thought:

1. Shut down the computer.
2. Document the hardware configuration of the system.
3. Transport the computer system to a secure location.
4. Make bit stream backups of hard disks and floppy disks.
5. Mathematically authenticate data on all storage devices.
6. Document the system date and time.
7. Make a list of key search words.
8. Evaluate the Windows swap file.
9. Evaluate file slack.
10. Evaluate unallocated space (erased files).
11. Search files, file slack, and unallocated space for keywords.
12. Document file names, dates, and times.
13. Identify file, program, and storage anomalies.
14. Evaluate program functionality.
15. Document your findings.
16. Retain copies of software used [2].

CAUTION

If you are not trained and have had a computer incident or threat, see sidebar, "Emergency Guidelines."

EMERGENCY GUIDELINES

The popularity of desktop and notebook computers has come with a mixed blessing. These wonderful tools contribute to increased productivity and help facilitate

→

communications and file transfers worldwide over the Internet. However, they also provide opportunities for abuse of corporate policies and the commission of computer-related crimes. Internet viewing of pornography has become a serious problem for corporations and government agencies. Embezzlements using computers have become commonplace in small- and medium-size businesses.

Computer forensic tools and techniques can help identify such abuses. They can also be used to find and document evidence in a civil or criminal case. However, the computer evidence must be preserved and protected. As a result, it is important that things are done correctly as soon as a computer incident is identified. By following the guidelines listed here, you stand a good chance of preserving the evidence:

1. Don't turn on or operate the subject computer.
2. Don't solicit the assistance of the resident "computer expert."
3. Don't evaluate employee email unless corporate policy allows it.

NOTE

Computer evidence is very fragile and can easily be altered or destroyed if the wrong things are done.

DON'T TURN ON OR OPERATE THE SUBJECT COMPUTER

The computer should first be backed up using bit stream backup software. When the computer is run, the potential exists for information in the Windows swap file to be overwritten. Internet activity and fragments of Windows work sessions exist in the Windows swap file. This can be valuable from an evidence standpoint. For that matter, the same is true of a Windows system. To save grief, don't run the computer.

DON'T SOLICIT THE ASSISTANCE OF THE RESIDENT COMPUTER EXPERT

The processing of computer evidence is tricky to say the least. Without proper training, even a world-class computer scientist can do the wrong things. Like any other science, computer science has its areas of specialty. Computer forensics investigators typically get calls *after the fact* and are informed that a computer-knowledgeable internal auditor or systems administrator has attempted to process a computer for evidence. In some cases, valuable evidence is lost or the evidence is so tainted that it loses its evidentiary value. For these reasons, seek the assistance of a computer specialist who has been trained in computer evidence processing procedures. Do this before you turn on the computer.

→

Don't Evaluate Employee Email Unless Corporate Policy Allows It

New electronic privacy laws [3] protect the privacy of electronic communications. If your corporate policy specifically states that all computers and data stored on them belongs to the corporation, then you are probably on safe ground. However, be sure that you have such a policy and that the employee involved has read the policy. Furthermore, it is always a good idea to check with corporate counsel. Don't be in a hurry; do things by the book. To do otherwise could subject you and your corporation to a lawsuit [4].

Shut Down the Computer

Depending on the computer operating system, this usually involves pulling the plug or shutting down a network computer using relevant commands required by the network involved. At the option of the computer investigator, pictures of the screen image can be taken. However, consideration should be given to possible destructive processes that may be operating in the background. These can be in memory or available through a connected modem. Depending on the operating system involved, a password-protected screen saver may also kick in at any moment. This can complicate the shutdown of the computer. Generally, time is of the essence, and the computer system should be shut down as quickly as possible.

Document the Hardware Configuration of the System

It is assumed that the computer system will be moved to a secure location where a proper chain of custody can be maintained and evidence processing can begin. Before dismantling the computer, it is important that pictures are taken of the computer from all angles to document the system hardware components and how they are connected. Labeling each wire is also important, so that it can easily be reconnected when the system configuration is restored to its original condition at a secure location.

Transport the Computer System to a Secure Location

This may seem basic, but all too often seized computers are stored in less than secure locations. War stories can be told about this one that relate to both law enforcement agencies and corporations. It is imperative that the subject computer is treated as evidence and stored out of reach of curious computer users. All too often, individuals operate seized computers without knowing that they are destroying potential evidence and the chain of custody. Furthermore, a seized computer left unattended can easily be compromised. Evidence can be planted on it and crucial evidence can be intentionally destroyed. A lack of a proper chain of custody can make a savvy defense attorney's day. Lacking a proper chain of custody, how can you say that relevant evidence was not planted on the computer after the seizure? The answer is that you cannot. Don't leave the computer unattended unless it is locked up in a secure location.

Make Bit Stream Backups of Hard Disks and Floppy Disks

The computer should not be operated, and computer evidence should not be processed until bit stream backups have been made of all hard disk drives and floppy disks. All evidence processing should be done on a restored copy of the bit stream backup rather than on the original computer. The original evidence should be left untouched unless compelling circumstances exist. Preservation of computer evidence is vitally important. It is fragile and can easily be altered or destroyed. Often such alteration or destruction of data is irreversible. Bit stream backups are much like an insurance policy and are essential for any serious computer evidence processing.

Mathematically Authenticate Data on All Storage Devices

You want to be able to prove that you did not alter any of the evidence after the computer came into your possession. Such proof will help you rebut allegations that you changed or altered the original evidence. Since 1989, law enforcement and military agencies have used a 32-bit mathematical process to do the authentication process. Mathematically, a 32-bit validation is accurate to approximately one in 4.3 billion. However, given the speed of today's computers and the vast amount of storage capacity on today's computer hard disk drives, this level of accuracy is no longer accurate enough. A 32-bit CRC can be compromised.

Document the System Date and Time

The dates and times associated with computer files can be extremely important from an evidence standpoint. However, the accuracy of the dates and times is just as important. If the system clock is one hour slow because of daylight-savings time, then file timestamps will also reflect the wrong time. To adjust for these inaccuracies, documenting the system date and time settings at the time the computer is taken into evidence is essential.

Make a List of Key Search Words

Because modern hard disk drives are so voluminous, it is all but impossible for a computer specialist to manually view and evaluate every file on a computer hard disk drive. Therefore, state-of-the-art automated forensic text search tools are needed to help find the relevant evidence. Usually some information is known about the allegations, the computer user, and the alleged associates who may be involved. Gathering information from individuals familiar with the case to help compile a list of relevant keywords is important. Such keywords can be used in the search of all computer hard disk drives and floppy diskettes using automated software. Keeping the list as short as possible is important and you should avoid using common words or words that make up part of other words. In such cases, the words should be surrounded with spaces.

Evaluate the Windows Swap File

The Windows swap file is a potentially valuable source of evidence and leads. In the past, this tedious task was done with hex editors, and it took days to evaluate just one Windows swap file. With the use of automated tools, this process now takes only a few minutes. When Windows 2000, XP, and 2003 are involved, the swap file may be set to be dynamically created as the computer is operated. This is the default setting, and when the computer is turned off, the swap file is erased. However, all is not lost, because the content of the swap file can easily be captured and evaluated.

Evaluate File Slack

File slack is a data storage area of which most computer users are unaware [5]. It is a source of significant *security leakage* and consists of raw memory dumps that occur during the work session as files are closed. The data dumped from memory ends up being stored at the end of allocated files, beyond the reach or view of the computer user. Specialized forensic tools are required to view and evaluate the file slack; file slack can provide a wealth of information and investigative leads. Like the Windows swap file, this source of ambient data can help provide relevant keywords and leads that may have previously been unknown.

On a well-used hard disk drive, as much as 1.1 billion bytes of storage space may be occupied by file slack. File slack should be evaluated for relevant keywords to supplement the keywords identified in the previous steps. Such keywords should be added to the computer investigator's list of keywords for use later. Because of the nature of file slack, specialized and automated forensic tools are required for evaluation. File slack is typically a good source of Internet leads. Tests suggest that file slack provides approximately 80 times more Internet leads than the Windows swap file. Therefore, this source of potential leads should not be overlooked in cases involving possible Internet uses or abuses.

Evaluate Unallocated Space (Erased Files)

On a well-used hard disk drive, billions of bytes of storage space may contain data associated with previously erased files. Unallocated space should be evaluated for relevant keywords to supplement the keywords identified in the previous steps. Such keywords should be added to the computer investigator's list of keywords for use in the next processing step. Because of the nature of data contained in unallocated space and its volume, specialized and automated forensic tools are required for evaluation. Unallocated space is typically a good source of data that was previously associated with word processing temporary files and other temporary files created by various computer applications.

Search Files, File Slack, and Unallocated Space for Keywords

The list of relevant keywords identified in the previous steps should be used to search all relevant computer hard disk drives and floppy diskettes. Several forensic text search utilities are available in the marketplace. Some of these tools are designed to be state-of-the-art and have been validated as security review tools by the federal government intelligence agencies.

It is important to review the output of the text search utility and equally important to document relevant findings. When relevant evidence is identified, the fact should be noted and the identified data should be completely reviewed for additional keywords. When new keywords are identified, they should be added to the list, and a new search should be conducted using the text search utility. Text search utilities can also be used effectively in security reviews of computer storage media.

Document File Names, Dates, and Times

From an evidence standpoint, file names, creation dates, and last modified dates and times can be relevant. Therefore, it is important to catalog all allocated and "erased" files. The file should be sorted based on the file name, file size, file content, creation date, and last modified date and time. Such sorted information can provide a timeline of computer usage. The output should be in the form of a word-processing-compatible file that can be used to help document computer evidence issues tied to specific files.

Identify File, Program, and Storage Anomalies

Encrypted, compressed, and graphic files store data in binary format. As a result, text data stored in these file formats cannot be identified by a text search program. Manual evaluation of these files is required and, in the case of encrypted files, much work may be involved. Depending on the type of file involved, the contents should be viewed and evaluated for its potential as evidence.

Reviewing the partitioning on seized hard disk drives is also important. When hidden partitions are found, they should be evaluated for evidence and their existence should be documented. If Windows 2000, XP, and 2003 are involved, it makes sense to evaluate the files contained in the Recycle Bin. The Recycle Bin is the repository of files selected for deletion by the computer user. The fact that they have been selected for deletion may have some relevance from an evidentiary standpoint. If relevant files are found, the issues involved should be documented thoroughly.

Evaluate Program Functionality

Depending on the application software involved, running programs to learn their purpose may be necessary. When destructive processes that are tied to relevant evidence are discovered, this can be used to prove willfulness. Such destructive processes can be tied to *hot keys* or the execution of common operating commands tied to the operating system or applications.

Document Your Findings

As indicated in the preceding steps, it is important to document your findings as issues are identified and as evidence is found. Documenting all of the software used in your forensic evaluation of the evidence, including the version numbers of the programs used, is also important. Be sure you are legally licensed to use the forensic software. Software pirates do not stand up well under the rigors of a trial. Smart defense lawyers will usually question software licensing; you don’t want to testify that you used unlicensed software in the processing of computer evidence. Technically, software piracy is a criminal violation of federal copyright laws.

When appropriate, mention in your documentation that you are licensed to use the forensic software involved. Screen prints of the operating software also help document the version of the software and how it was used to find or process the evidence.

Retain Copies of Software Used

Finally, as part of your documentation process, it is recommended that a copy of the software used be included with the output of the forensic tool involved. Normally, this is done on an archive Zip disk, Jazz disk, or other external storage device (external hard disk drive). When this documentation methodology is followed, it eliminates confusion (about which version of the software was used to create the output) at trial time. Often it is necessary to duplicate forensic-processing results during or before trial. Duplication of results can be difficult or impossible to achieve if the software has been upgraded and the original version used was not retained.

NOTE

There is a high probability that you will encounter this problem because most commercial software is upgraded routinely, but it may take years for a case to go to trial.

LEGAL ASPECTS OF COLLECTING AND PRESERVING COMPUTER FORENSIC EVIDENCE

Some of the most common reasons for improper evidence collection are poorly written policies, lack of an established incident response plan, lack of incident response training, and a broken chain of custody. For the purposes of this chapter, the reader should assume that policies have been clearly defined and reviewed by legal counsel, an incident response plan is in place, and necessary personnel have been properly trained. The remainder of this chapter focuses on the procedure a private organization should follow in collecting computer forensic evidence to maintain chain of custody.

Definition

In simple terms, a chain of custody is a roadmap that shows how evidence was collected, analyzed, and preserved in order to be presented as evidence in court. Establishing a clear chain of custody is crucial because electronic evidence can be easily altered. A clear chain of custody demonstrates that electronic evidence is trustworthy. Preserving a chain of custody for electronic evidence, at a minimum, requires proving that:

- No information has been added or changed.
- A complete copy was made.
- A reliable copying process was used.
- All media was secured [6].

NOTE

Proving this chain is unbroken is a prosecutor's primary tool in authenticating electronic evidence.

Legal Requirements

When evidence is collected, certain legal requirements must be met. These legal requirements are vast, complex, and vary from country to country. However, there are certain requirements that are generally agreed on within the United States. U.S. Code Title 28, Section 1732 provides that log files are admissible as evidence if they are collected *in the regular course of business*. Also, Rule 803(6) of the Federal Rules of Evidence provides that logs, which might otherwise be considered hearsay, are admissible as long as they are collected *in the course of regularly conducted business activity*. This means you'd be much safer to log everything all the time and deal with the storage issues than to turn on logging only after an incident is suspected. Not only is this a bit like closing the barn door after the horse has fled, but it may also render your logs inadmissible in court.

Another factor in the admissibility of log files is the ability to prove that they have not been subject to tampering. Whenever possible, digital signatures should be used to verify log authenticity. Other protective measures include, but are not limited to, storing logs on a dedicated logging server and encrypting log files. Log files are often one of the best, if not only, sources of evidence available. Therefore, due diligence should be applied in protecting them.

One other generally accepted requirement of evidence collection is a user's expectation of privacy. A key to establishing that a user has no right to privacy when using corporate networks or computer systems is the implementation of a log-on banner. CERT Advisory CA-1992-19 suggests the following text be tailored to a corporation's specific needs under the guidance of legal counsel:

- This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.
- In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.
- Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Furthermore, security policy can play a key role in establishing a user's expectation of privacy. The Supreme Court ruling in O'Connor v. Ortega, 480 U.S. 709 (1987) implies that the legality of workplace monitoring depends primarily on whether employment policies exist that authorize monitoring and whether that policy has been clearly communicated to employees. To prove that the policy has been communicated, employees should sign a statement indicating that they have read, understood, and agreed to comply with corporate policy and consent to system monitoring.

Evidence Collection Procedure

When the time arrives to begin collecting evidence, the first rule that must be followed is *do not rush*. Tensions will probably be high and people will want to find answers as quickly as possible. However, if the investigators rush through these procedures, mistakes will be made and evidence will be lost.

The investigation team will need to bring certain tools with them to the incident site. They will need a copy of their incident-handling procedure, an evidence collection notebook, and evidence identification tags. Depending on the type of incident and whether the team will be able to retrieve an entire system or just the data, they may also need to bring tools to produce reliable copies of electronic evidence, including media to use in the copying process. In some cases, legal counsel will want photographs of the system prior to search and seizure. If this is something your legal counsel wants as part of the evidence, then also include a Polaroid camera in the list of tools.

Policy and procedure should indicate who is to act as incident coordinator. When an incident is reported, this individual will contact the other members of the response team as outlined in the Incident Response Policy. Upon arrival at the incident site, this individual will be responsible for ensuring that every detail of the incident-handling procedure is followed. The incident coordinator will also assign team members the various tasks outlined in the incident-handling procedure and will serve as the liaison to the legal team, law enforcement officials, management, and public relations personnel. Ultimate responsibility for ensuring that evidence is properly collected and preserved, and that the chain of custody is properly maintained, belongs to the incident coordinator.

One team member will be assigned the task of maintaining the evidence notebook. This person will record the who, what, where, when, and how of the investigation process. At a minimum, items to be recorded in the notebook include

- Who initially reported the suspected incident along with time, date, and circumstances surrounding the suspected incident.
- Details of the initial assessment leading to the formal investigation.
- Names of all persons conducting the investigation.
- The case number of the incident.
- Reasons for the investigation.
- A list of all computer systems included in the investigation, along with complete system specifications. Also include identification tag numbers assigned to the systems or individual parts of the system.
- Network diagrams.
- Applications running on the computer systems previously listed.

- A copy of the policy or policies that relate to accessing and using the systems previously listed.
- A list of administrators responsible for the routine maintenance of the system.
- A detailed list of steps used in collecting and analyzing evidence. Specifically, this list needs to identify the date and time each task was performed, a description of the task, who performed the task, where the task was performed, and the results of the analysis.
- An access control list of who had access to the collected evidence at what date and time [6].

NOTE

A separate notebook should be used for each investigation. Also, the notebook should not be spiral-bound. It should be bound in such a way that it is obvious if a page or pages have been removed.

This notebook is a crucial element in maintaining chain of custody. Therefore, it must be as detailed as possible to assist in maintaining this chain.

Another team member (or members) will be assigned the task of evidence collection. To avoid confusion, the number of people assigned this task should be kept to a minimum. This member (or members) should also be highly proficient with copying and analysis tools. This person will tag all evidence and work with the person responsible for the evidence notebook to ensure that this information is properly recorded. Next, the person will also be responsible for making a reliable copy of all data to be used as evidence. The data will include complete copies of drives on compromised or suspect systems, as well as all relevant log files. This can be done on-site or the entire system can be moved to a forensics lab, as needs dictate.

A simple file copy is not sufficient to serve as evidence in the case of compromised or suspect systems. A binary copy of the data is the proper way to preserve evidence.

NOTE

A reliable copy process has three critical characteristics. First, the process must meet industry standards for quality and reliability. This includes the software used to create the copy and the media on which the copy is made. A good benchmark is whether the software is used and relied on by law enforcement agencies. Second, the copies must be capable of independent verification. Third, the copies must be tamperproof.

Two copies of the data should be made using an acceptable tool. The original should be placed in a sealed container. One copy will be used for analysis and the other copy can be put back in the system so the system can be returned to service as quickly as possible.

NOTE *In certain cases, it is necessary to keep the entire system or certain pieces of hardware as part of evidence. The investigation coordinator will work with the legal team to determine the requirements for a given case.*

Once all evidence is collected and logged, it can be securely transported to the forensics lab. A detailed description of how data was transported and who was responsible for the transport, along with date, time, and route, should be included in the log. It is required that the evidence be transported under dual control.

Storage and Analysis of Data

Finally, the chain of custody must be maintained throughout the analysis process. One of the keys to maintaining the chain is a secure storage location. If the corporation uses access control cards or video surveillance in other parts of the building, consider using these devices in the forensics lab. Access control cards for entering and exiting the lab will help verify who had access to the lab at what time. The video cameras will help determine what they did once they were inside the lab. At a minimum, the lab must provide some form of access control; a log should be kept detailing entrance and exit times of all individuals. It is important that evidence never be left in an unsecured area. If a defense lawyer can show that unauthorized persons had access to the evidence, it could easily be declared inadmissible.

Pieces of evidence should be grouped and stored by case along with the evidence notebook. In an effort to be as thorough as possible, investigators should follow a clearly documented analysis plan. A detailed plan will help prevent mistakes (which could lead to the evidence becoming inadmissible) during analysis. As analysis of evidence is performed, investigators must log the details of their actions in the evidence notebook. The following should be included at a minimum:

- The date and time of analysis
- Tools used in performing the analysis
- Detailed methodology of the analysis
- Results of the analysis [6]

Again, the information recorded in the evidence notebook must be as detailed as possible to demonstrate its trustworthiness. A trial lawyer well versed in the technological world, who knows how to ask the right questions, may find that the *method or circumstances of preparation indicate lack of trustworthiness* (under Fed. R. Evid. 803(6)), to such a degree that a court will sustain, or at least consider, a challenge to the admissibility of the evidence. A properly prepared evidence notebook will help to defeat such a challenge.

Finally, once all evidence has been analyzed and all results have been recorded in the evidence notebook, a copy of the notebook should be made and given to the legal team. If the legal team finds that sufficient evidence exists to take legal action, it will be important to maintain the chain of custody until the evidence is handed over to the proper legal authorities. Legal officials should provide a receipt detailing all of the items received for entry into evidence.

SUMMARY

The latter part of the 20th century was marked by the electronic transistor and the machines and ideas made possible by it. As a result, the world changed from analog to digital. Although the computer reigns supreme in the digital domain, it is not the only digital device. An entire constellation of audio, video, communications, and photographic devices are becoming so closely associated with the computer as to have converged with it.

From a law enforcement perspective, more of the information that serves as currency in the judicial process is being stored, transmitted, or processed in digital form. The connectivity resulting from a single world economy, in which the companies providing goods and services are truly international, has enabled criminals to act transjurisdictionally with ease. Consequently, a perpetrator may be brought to justice in one jurisdiction while the digital evidence required to successfully prosecute the case may only reside in other jurisdictions.

This situation requires that all nations have the ability to *collect and preserve digital evidence* for their own needs as well as for the potential needs of other sovereigns. Each jurisdiction has its own system of government and administration of justice, but in order for one country to protect itself and its citizens, it must be able to make use of evidence collected by other nations. Though it is not reasonable to expect all nations to know about and abide by the precise laws and rules of other countries, a means that will allow the exchange of evidence must be found. This chapter was a first attempt to define the technical aspects of these exchanges.

Conclusions

- The laws surrounding the collection and preservation of evidence are vast and complex.
- Even if local law enforcement does not have a computer forensics expert on staff, they will know the basic rules of evidence collection and should have con-

tacts within the law enforcement community who are experts in computer forensics.

- A clearly documented plan is essential for an investigation team to be successful in collecting admissible evidence. The plan should be designed with the assistance of legal counsel and law enforcement agencies to ensure compliance with all applicable local, state, and federal laws.
- Once a plan has been drafted and the incident team is assembled, practice should begin.
- Configure a test network in a lab environment and invite members of the IT staff to attempt to circumvent the security measures installed in the lab network.
- Treat the intrusion as an actual incident and follow incident handling and evidence collection procedures.
- Review the results with the team and evaluate whether evidence collected would be admissible, based on the procedures followed and the analysis results.
- When possible, include legal staff and local law enforcement in practice sessions.
- When in doubt, hire an expert.
- If resident security staff members are not equipped to perform the investigation, do not hesitate to bring in outside assistance.
- It is in the best interest of the company to ensure that the investigation is handled properly.
- The goal is to collect and preserve evidence in such a way that it will be admissible in a court of law.

An Agenda for Action

When completing the Duplication and Preservation of Digital Evidence Checklist (Table F7.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for duplication and preservation of digital evidence. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let’s move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? The computer investigator needs to be worried about destructive process and devices being planted by the computer owner but does not need to be concerned about the operating system of the computer and applications.
2. True or False? Computer evidence is fragile by its very nature and the problem is compounded by the potential of destructive programs and open data.
3. True or False? Some of the least common reasons for improper evidence collection are poorly written policies, lack of an established incident response plan, lack of incident response training, and a broken chain of custody.
4. True or False? The complexity of criminal law means that the overwhelming majority of cases do not make it to civil or criminal court, but should.
5. True or False? If your preservation is good, it becomes fairly evident that your collection and transportation of evidence gives rise to numerous possibilities for error in the form of destruction, mishandling, and contamination.

Multiple Choice

1. There are three criminal evidence rules to gain admissibility, except for two:
   A. Destruction
   B. Mishandling
   C. Authentication
   D. The best evidence rule
   E. Exceptions to the hearsay rule
2. The following general computer evidence processing steps have been provided, except:
   A. Shut down the computer.
   B. Document the hardware configuration of the system.
   C. Transport the computer system to an unsecure location.
   D. Make bit stream backups of hard disks and floppy disks.
   E. Mathematically authenticate data on all storage devices.
3. By following the guidelines listed here, you stand a good chance of preserving the evidence, except for two:
   A. Turn on or operate the subject computer.
   B. Don’t turn on or operate the subject computer.
   C. Don’t solicit the assistance of the resident “computer expert.”

D. Solicit the assistance of the resident “computer expert.”
E. Don’t evaluate employee email unless corporate policy allows it.

4. Preserving a chain of custody for electronic evidence, at a minimum, requires proving that, except:

A. No information has been added or changed.
B. A complete copy was made.
C. A reliable copying process was used.
D. An unreliable copying process was used.
E. All media was secured.

5. One team member will be assigned the task of maintaining the evidence notebook. This person will record the who, what, where, when, and how of the investigation process. At a minimum, items to be recorded in the notebook include the following, except:

A. Who initially declined to report the suspected incident along with time, date, and circumstances surrounding the suspected incident
B. Details of the initial assessment leading to the formal investigation
C. Names of all persons conducting the investigation
D. The case number of the incident
E. Reasons for the investigation

Exercise

Downsizing and outsourcing overseas at a large U.S. government contractor resulted in the termination of 500 engineers. What would the role of a CFS team (CFST) be here?

HANDS-ON PROJECTS

A male employee at a regional trucking company was accused of downloading child pornography to his office computer. He is now suing the company for millions for being wrongly accused, which resulted in tarnishing his reputation and his standing in the community. How did the CFS prove that the employee did not download the images, and in fact some other employee did?

Case Project

A computer was seized during a routine drug arrest. What did the CFS do to prove that the computer was involved in other crimes?

Optional Team Case Project

A small landscaping company suspecting embezzlement hired a CFST to review their bookkeeper’s computer. Explain how a CFST would deal with this case.

REFERENCES

[1] "Digital Evidence Collection & Handling" (© North Carolina Wesleyan College), North Carolina Wesleyan College, 3400 N. Wesleyan Boulevard, Rocky Mount, NC 27804, 2004.

[2] Computer Evidence Processing Steps," New Technologies, Inc., 2075 NE Division St., Gresham, Oregon 97030, 2001.

[3] Vacca, John R., *Net Privacy: A Guide to Developing and Implementing an Ironclad E-Business Privacy Plan,* McGraw-Hill Professional, New York, 2001.

[4] "Computer Incident Response Guidelines," New Technologies, Inc., 2075 NE Division St., Gresham, Oregon 97030, 2001.

[5] Vacca, John R., *The Essential Guide to Storage Area Networks,* Prentice Hall, New York, 2002.

[6] Witter, Franklin, "Legal Aspects of Collecting and Preserving Computer Forensics Evidence," Branch Banking & Trust, 2501 Wooten Blvd., MC 100-99-08-25, Wilson, North Carolina 27893 (SANS Institute, 5401 Westbard Ave., Suite 1501, Bethesda, MD 20816), 2001.

8 Computer Image Verification and Authentication

As law enforcement and other computer forensics investigators become more familiar with handling evidential computer material, it is apparent that a number of more or less formalized procedures have evolved to maintain both the continuity and integrity of the material to be investigated. Although these procedures are extremely effective under the current rules of evidence, it is expected that alternative procedures will develop as technology advances. The current procedures, in use by both law enforcement and computer forensics investigators, work something like this:

At least two copies are taken of the evidential computer. One of these is sealed in the presence of the computer owner and then placed in secure storage. This is the master copy and it will only be opened for examination under instruction from the court in the event of a challenge to the evidence presented after forensic analysis on the second copy. If the computer has been seized and held in secure storage by law enforcement, this will constitute *best evidence*. If the computer has not been seized, then the master copy becomes best evidence. In either case, the assumption is that while in secure storage, there can be no possibility of tampering with the evidence. This does not protect the computer owner from the possibility that secured evidence may be tampered with.

A growing practical problem with this method of evidential copying occurs not because of the security aspect or appearance of the situation, but because of the increasing sizes of fixed disks found in computers. A size of 2 gigabytes is no longer unusual, and it is common to find more than one fixed disk within a single machine. The cost of the media is decreasing slowly, but this is still significant when considering the quantity of information to be copied and stored (even though the system does allow for media reuse). There is also the problem of the length of time individual copies may take to complete. A sizable saving in both time and expense might, therefore, be achieved if an alternative method of evidential security could be arranged.

SPECIAL NEEDS OF EVIDENTIAL AUTHENTICATION

A wealth of mathematical algorithms deal with secure encryption, verification, and authentication of computer-based material. These display varying degrees of security and complexity, but all of them rely on a *second channel* of information, whereby certain elements of the encryption/decryption/authentication processes are kept secret. This is characterized most plainly in the systems of public and private key encryption but is also apparent in other protocols.

Consider the investigative process where computers are concerned. During an investigation, it is decided that evidence may reside on a computer system. It may be possible to seize or impound the computer system, but this risks violating the basic principle of *innocent until proven guilty*, by depriving an innocent party of the use of his or her system. It should be perfectly possible to copy all the information from the computer system in a manner that leaves the original system untouched and yet makes all contents available for forensic analysis.

When this is done, the courts may rightly insist that the copied evidence is protected from either accidental or deliberate modification and that the investigating authority should prove that this has been done. Thus, it is not the content that needs protection, but its integrity.

This protection takes two forms: a secure method of determining that the data has not been altered by even a single bit since the copy was taken and a secure method of determining that the copy is genuinely the one taken at the time and on the computer in question. For the purpose of this chapter, these elements are collectively referred to here as the digital image verification and authentication protocol [1].

It is argued that when considering forensic copies of computer contents, encryption of data is not the point at issue. Neither are the provisions of the many digital signature protocols appropriate to the requirements of evidential authentication (see sidebar, “Digital IDs and Authentication Technology”).

DIGITAL IDS AND AUTHENTICATION TECHNOLOGY

When customers buy software in a store, the source of that software is obvious. Customers can tell who published the software and they can see whether the package has been opened. These factors enable customers to make decisions about what software to purchase and how much to “trust” those products.

→

When customers download software from the Internet, the most they see is a message warning them about the dangers of using the software. The Internet lacks the subtle information provided by packaging, shelf space, shrink wrap, and the like. Without an assurance of the software's integrity, and without knowing who published the software, it's difficult for customers to know how much to trust software. It's difficult to make the choice of downloading the software from the Internet.

For example (when using Microsoft Authenticode coupled with Digital IDs™ from VeriSign®), through the use of digital signatures, software developers are able to include information about themselves and their code with their programs. When customers download software signed with Authenticode and verified by VeriSign, they should be assured of *content source*, indicating that the software really comes from the publisher who signed it, and *content integrity,* indicating that the software has not been altered or corrupted since it was signed.

NOTE *The author and publisher do not endorse any specific computer forensics software over another. Authenticode from Microsoft and Digital IDs from VeriSign are mentioned here for illustration purposes only.*

Users benefit from this software accountability because they know who published the software and that the code hasn't been tampered with. In the extreme case that software performs unacceptable or malicious activity on their computers, users can pursue recourse against the publisher. This accountability and potential recourse serve as a strong deterrent to the distribution of harmful code.

Developers and Webmasters should benefit from Authenticode, because it puts trust in their name and makes their products harder to falsify. By signing code, developers build a trusted relationship with users, who then learn to confidently download signed software from that software publisher or Web site provider. With Authenticode, users can make educated decisions about what software to download, knowing who published the software and that it hasn't been tampered with.

WHO NEEDS A SOFTWARE PUBLISHER ID?

Any publisher who plans to distribute code or content over the Internet or over corporate extranets, risks impersonation and tampering. For example, Authenticode is currently used to sign 32-bit .exe files (portable executable files), .cab files, .ocx files, and .class files. In particular, if you are distributing active content (such as ActiveX controls) for use with such Microsoft end user applications as Internet Explorer, Exchange, Outlook, or Outlook Express, you will want to sign code using Authenticode.

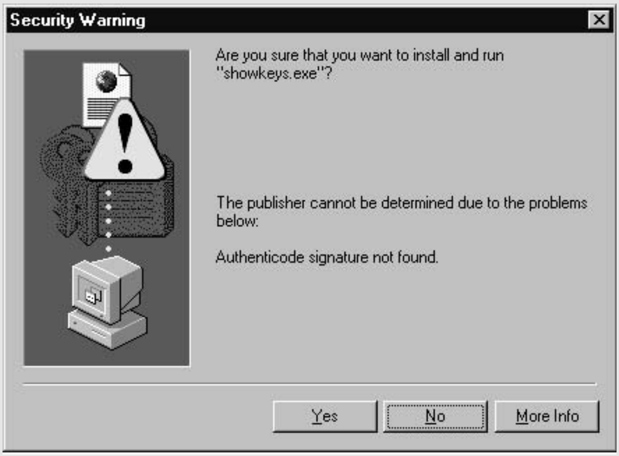
→

VeriSign offers a Class 3 Digital ID designed for commercial software publishers. These are companies and other organizations that publish software. This class of digital IDs provides the identity of a publishing organization and is designed to represent the level of assurance provided today by retail channels for software.

What Authenticode Looks Like to Consumers

Microsoft client applications, such as Internet Explorer, Exchange, Outlook, and Outlook Express, come with security features that incorporate Authenticode. These applications are often used to obtain other pieces of software. In a component model such as Active™ or Java™ this happens frequently, often without the end user being aware of it. For example, when a user visits a Web page that uses executable files to provide animation or sound, code is often downloaded to the end user's machine to achieve the effects. Although this may provide substantial value, users risk downloading viruses or code from a disreputable publisher.

If an end user of one of these applications encounters an unsigned component distributed via the Internet, the following will occur: if the application's security settings are set on High, the client application will not permit the unsigned code to load; if the application's security settings are set on Medium, the client application will display a warning similar to the screen shown in Figure 8.1 [2].


Security Warning

Are you sure that you want to install and run "showkeys.exe"?

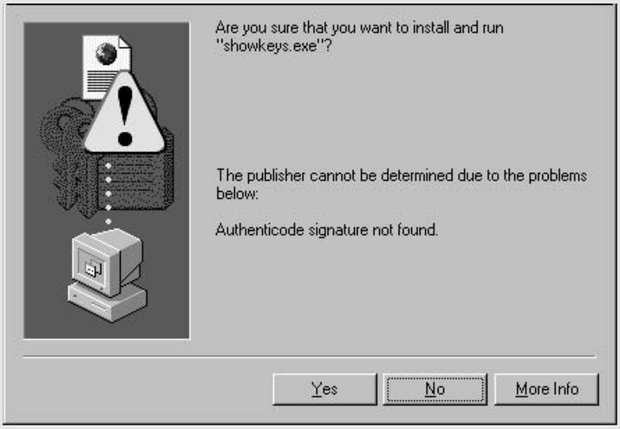
The publisher cannot be determined due to the problems below:

Authenticode signature not found.

FIGURE 8.1 Security warning screen.

→

By contrast, if a user encounters a signed applet or other code, the client application will display a screen similar to the one shown in Figure 8.2 [2]. Through Authenticode, the user is informed:



Are you sure that you want to install and run "showkeys.exe"?

The publisher cannot be determined due to the problems below:

Authenticode signature not found.

FIGURE 8.2 Client application security warning.

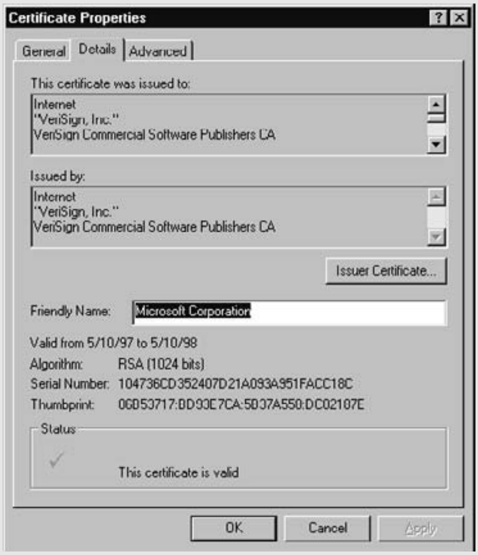
- Of a place to find out more about the control
- The authenticity of the preceding information

Users can choose to trust all subsequent downloads of software from the same publisher. They can also choose to trust all software published by commercial publishers (see preceding information) that has been certified by VeriSign. Simply by clicking the More Info button, users can inspect the certificate and verify its validity, as shown in Figure 8.3 [2].

TECHNICAL OVERVIEW

A digital ID (also known as a digital certificate) is a form of electronic credentials for the Internet. Similar to a driver's license, employee ID card, or business license, a digital ID is issued by a trusted third party to establish the identity of the ID holder. The third party who issues certificates is known as a certification authority (CA).

Digital ID technology is based on the theory of public key cryptography. In public key cryptography systems, every entity has two complementary keys (a public key and a private key) that function only when they are held together. Public keys are widely distributed to users, whereas private keys are kept safe and only used by their owner. Any code digitally signed with the publisher's private key can only be successfully verified using the complementary public key. Another way to look at this is



This certificate was issued to:
Internet
"VeriSign, Inc."
VeriSign Commercial Software Publishers CA

Issued by:
Internet
"VeriSign, Inc."
VeriSign Commercial Software Publishers CA

Friendly Name: Microsoft Corporation

Valid from 5/10/97 to 5/10/98
Algorithm: RSA (1024 bits)
Serial Number: 104736CD352407D21A093A951FACC18C
Thumbprint: 06D53717:DD93E7CA:5037A550:DC02107E

Status
✓ This certificate is valid

FIGURE 8.3 Inspect the certificate and verify its validity.

that code successfully verified using the publisher's public key (which is sent along with the digital signature), could only have been digitally signed using the publisher's private key (thus authenticating the source of the code) and has not been tampered with.

The purpose of a digital ID is to reliably link a public and private key pair with its owner. When a CA such as VeriSign issues digital IDs, it verifies that the owner is not claiming a false identity. Just as when a government issues you a passport, it is officially vouching for the fact that you are who you say you are. Thus, when a CA issues you a digital certificate, it is putting its name behind the statement that you are the rightful owner of your public and private key pair.

Certification Authorities

CAs such as VeriSign are organizations that issue digital certificates to applicants whose identity they are willing to vouch for. Each certificate is linked to the certificate of the CA that signed it. As the Internet's leading CA, VeriSign has the following responsibilities:

- Publishing the criteria for granting, revoking, and managing certificates
- Granting certificates to applicants who meet the published criteria
- Managing certificates (enrolling, renewing, and revoking them)
- Storing VeriSign's root keys in an exceptionally secure manner
- Verifying evidence submitted by applicants

→

- Providing tools for enrollment
- Accepting the liability associated with these responsibilities
- Timestamping digital signatures

How Authenticode Works with VeriSign Digital IDs

Authenticode relies on industry-standard cryptography techniques such as X.509 v3 or higher certificates and PKCS #7 and #10 signature standards. These are well-proven cryptography protocols, which ensure a robust implementation of code-signing technology. Developers can use the WinVerifyTrust API, on which Authenticode is based, to verify signed code in their own Win32 applications.

Authenticode uses digital signature technology to assure users of the origin and integrity of software. In digital signatures, the private key generates the signature, and the corresponding public key validates it. To save time, the Authenticode protocols use a cryptographic digest, which is a one-way hash of the document. The process is outlined below and shown in Figure 8.4 [2].

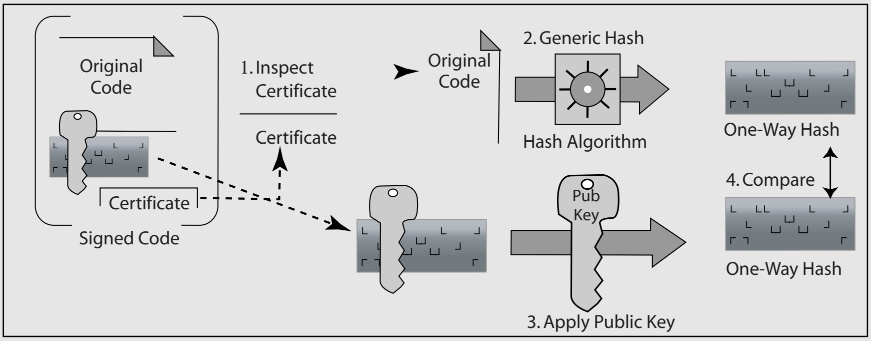


FIGURE 8.4 Authenticode: VeriSign Digital ID process.

1. Publisher obtains a software developer digital ID from VeriSign.
2. Publisher creates code
3. Using the SIGNCODE.EXE utility, the publisher
   a. Creates a hash of the code, using an algorithm such as MD5 or SHA
   b. Encrypts the hash using his private key
   c. Creates a package containing the code, the encrypted hash, and the publisher's certificate
4. The end user encounters the package.

→

5. The end user's browser examines the publisher's digital ID. Using the VeriSign® root public key, which is already embedded in Authenticode-enabled applications, the end user's browser verifies the authenticity of the software developer digital ID (which is itself signed by the VeriSign root Private Key).
6. Using the publisher's public key contained within the publisher's digital ID, the end user's browser decrypts the signed hash.
7. The end user's browser runs the code through the same hashing algorithm as the publisher, creating a new hash.
8. The end user's browser compares the two hashes. If they are identical, the browser messages that the content has been verified by VeriSign, and the end user has confidence that the code was signed by the publisher identified in the digital ID and that the code hasn't been altered since it was signed.

NOTE

The entire process is seamless and transparent to end users, who see only a message that the content was signed by its publisher and verified by VeriSign.

TIMESTAMPING

Because key pairs are based on mathematical relationships that can theoretically be "cracked" with a great deal of time and effort, it is a well-established security principle that digital certificates should expire. Your VeriSign Digital ID will expire one year after it is issued. However, most software is intended to have a lifetime of longer than one year. To avoid having to resign software every time your certificate expires, a timestamping service is now available. Now, when you sign code, a hash of your code will be sent to VeriSign to be timestamped. As a result, when your code is downloaded, clients will be able to distinguish between code signed with an expired certificate, which should not be trusted, and code signed with a certificate that was valid at the time the code was signed, but which has subsequently expired. This code should be trusted [2].

PRACTICAL CONSIDERATIONS

It is useful to present some fundamental requirements of a forensic data collection system before considering how these can be securely protected. These requirements were chosen to reflect the experience of computer forensic investigators. Other forensic experts may argue against some or all of them:

1. Forensic data collection should be complete and non-software specific, thus avoiding software traps and hidden partitioning.

2. In operation, it should be as quick and as simple as possible to avoid error or delay.
3. It should be possible for anyone to use a forensic data collection system with the minimum amount of training.
4. Necessary costs and resources should be kept to a minimum [1].

To meet the conditions specified in items 2, 3, and 4, the *digital integrity verification and authentication* protocol must be tailored to suit. For the collection phase to remain quick and simple, the digital integrity verification and authentication protocol must not add significantly to the time required for copying, nor should there be additional (possibly complex) procedures.

The time and effort required to introduce links with key management agencies, trusted third parties, key distribution centers, and similar paraphernalia of digital signatures and document authentication is not necessary. It would add to the cost and complexity with little increase to security. It might mean, for example, that only investigators issued with a valid digital signature would be able to complete copies. Who is to issue these? Where are they to be stored? How will each individual remember his or her own key? How can misuse of keys be detected?

The digital integrity verification and authentication protocol described in the next section is virtually a self-contained system. Obviously, a truly self-contained encryption system cannot be cryptographically secure. However, within the digital integrity verification and authentication protocol, alternative channels of security are used to provide a truly secure system, but at much lower cost in time and consumables.

PRACTICAL IMPLEMENTATION

The emphasis here is on a practical application of proven technology, such that a minimum amount of reliance is placed on the technical ability of the operator/investigator. It must be understood that during the copying process, procedures are implemented to trap and handle hardware errors, mapping exceptions where necessary. It must also be understood that procedures are implemented to verify that information is copied correctly. This information is stored on each cartridge within a copy series.

Also stored on each cartridge is a reference area containing copy-specific information such as CPU type and speed, hardware equipment indicators, copying drive serial number, cartridge sequence number, exhibit details and reference comments, operator name together with a unique password, and the real date and time as entered by the operator. The remainder (in fact the bulk) of each cartridge contains the information copied from the suspect drive on a sector by sector basis.

Thus, for computer forensics investigators and senior technology strategists, IT security with regard to image verification and authentication is a study in contrasts. On the one hand, it's a topic that chief information officers (CIOs) repeatedly cite as one of their most important issues, if not the most important. Yet, despite the 9-11-01 terrorist attacks, CIOs and senior IT executives still suggest that their non-IT colleagues simply do not share their sense of urgency—they have all become complacent. Perhaps that's because relatively few security breaches have hit their organizations—and most of those are of the *nuisance* variety, which doesn't cost a lot of hard dollars. Unfortunately, security is like insurance: You never know when you'll need it. With that in mind, let's take a look at why there isn't a sense of urgency in implementing image verification and authentication security considerations.

Security Considerations

Day after day, in every company, university, and government agency, a never-ending parry and thrust with those who threaten the security of their networks continues. Ultimately, with everything changing, the struggle for security is a constant battle. Everything has to be updated as new and different threats are received.

Organizations must be constantly vigilant. New technologies in the areas of image verification and authentication bring new vulnerabilities, and computer forensics investigators are constantly discovering vulnerabilities in old image verification and authentication products. It is expected that the number of vulnerabilities reported in 2002 will be triple the previous year's number.

As a result, CIOs are devoting more money and time to image verification and authentication security. The costs will continue to grow as the world becomes more interconnected and as the cleverness of those who would cause harm increases. In 1989, CERT/CC (*http://www.cert.org/*) counted fewer than 200 security incidents (other viruses since then, and everything that resulted from it, counts as one incident). In 2003, CERT/CC recorded more than 40,000 incidents.

The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. They study Internet security vulnerabilities, handle computer security incidents, publish security alerts, research long-term changes in networked systems, and develop information and training to help you improve security at your site.

No one is immune. When 30 computer security experts involved in a spare-time endeavor called The Honeynet Project hooked a typical computer network to the Internet to see what hackers would do, the network was probed and exploited in 15 minutes. Such hackers are intelligent adversaries who are going to find your weak points. That's what makes the Honeynet Project different from other kinds of risk management.

Network managers must balance security against the business advantages that new technology (image verification and authentication security) brings. The biggest issue most companies face is how to allow users to do everything they need to do to be efficient from a business standpoint without opening the door to an attack.

Most CIOs do understand the key role employees play in security. Some take precautions when employees are being dismissed—quickly removing their network access, for example. Everyone knows that education is key. Employees can definitely cause problems if they don't do the right thing.

Employees can also be allies in the battle. Most CIOs view their staff as a strength in their overall information security program. Staff members are the ones who make sure viruses don't come in and holes aren't created in the firewall. They have to understand that most business is built on trust, and their role in maintaining that trust is critical.

It's also necessary to win support of non-staff members. Usually it's not an issue, because, in the case of a virus outbreak, everybody is affected. It's very visible, and anything that is done is appropriate as far as the non-staff employees are concerned. Some esoteric things, such as virtual private network (VPN) hardware or encrypting outside communications, are a little harder to sell. The non-staff employees want to know what it's going to cost and what the risk is. Non-staff employees can understand it on a gut level, but after all, companies are not the Defense Department—they don't make nuclear arms; they roll and distribute stainless steel or other products.

For example, the CIO should create a team, consisting of him- or herself, the company's security officer, and the internal auditor, that meets regularly to review risks and then makes recommendations on spending. CERT/CC encourages technical and business-side people to work together because they will bring different perspectives to the matter. This collaboration should be part of an organization-wide, comprehensive plan to prevent companies from focusing on one aspect of security and overlooking others. Security is a mindset and a management practice as much as it is a technology.

Nevertheless, there is always some difficulty in enlisting the support of senior executives at some point. It's more political than technical. Full communication and credibility are important. You should not try to deal with problems unless there really are problems. You should also avoid affecting the user any more than is absolutely necessary.

Financial institutions have had to conform to the Gramm-Leach-Bliley Act of 1999, which governs these institutions and the privacy of their customer information [3]. Privacy is critical by law, and it's security that enables privacy. Financial institutions have to prove that they are securing their members' information. Financial institutions are also subject to at least an annual review. In the past it was "Show me your vaults, show me your cameras, show me your paper-shredders." Now it's "Show me your password policy, show me your firewall."

In the end, it's difficult, perhaps impossible, to measure the return on investment in security, but perhaps that's the wrong way to think about it. It's difficult to determine whether CIOs are overspending or under spending. You can't overspend, really. You have to protect your data. It only takes one time—one hacker getting in and stealing all your financial data. It would be irresponsible on a CIO's part to not have the toughest image verification and authentication security possible.

SUMMARY

The overall security of a computer image verification and authentication system rests in the combination of security measures. These can be summarized technically as follows:

- The block hash values are generated in conjunction with a one-time pad simulation. As well as providing continuity between blocks, this negates the redundancy encountered when copying the type of data found on fixed disks (quantities of zeroes, ASCII text, and fixed structures). Thus, repeat hash values are avoided and a possible birthday attack is thwarted.
- The encryption of the vault, because it only occurs at the end of each section of the copy, can be accomplished using a secure encryption algorithm.
- Both the prosecuting and defending parties have secure protection against the possibility of the evidence being tampered with as long as they retain the sealed floppies. In the event of a challenge, one or both envelopes can be opened in court and verified against each other and the cartridges. In the event of a mismatch with the cartridge, reference to the encrypted vault stored on the cartridge will show which block on the cartridge has been altered (or even the vault itself) [1].

Image verification and authentication security involves a relatively straightforward risk-management equation (the more security you put in place, the more onerous it is for end users), and until the technology arrives to make impenetrable security invisible to end users, it will remain that way. Most CIOs today clearly support increased security, and although they fault their non-IT cohorts for lack of security awareness, they appear to be realistic about the burden it puts on their companies' business units. However, CIOs aren't instituting enough of the high-profile risk-assessment measures that would increase awareness of the problem throughout their corporations.

Conclusions

- Having examined various alternative methods of copying suspect computers, a computer image verification and authentication concept with dedicated hardware remains the simplest, most secure, and most practical method currently available.
- Copying directly to CD-ROM is not possible without some buffer drive to enable correct data-streaming; this introduces a number of potential problem areas both with the increasingly complex hardware and evidential continuity.
- CD-ROM technology was originally developed for audio requirements, and the current reliability when storing digital data is extremely suspect [4].
- Copying to tape is less expensive, but the viability of data stored for long periods (in many cases years), particularly if unattended, is also extremely suspect. Both of these methods have additional problems of data verification during and after the copy process.
- Software-copying packages intended for use on nonspecific peripheral storage devices raise problems of technical support and hardware matching.
- The problems that were originally anticipated with rewriteable media have not materialized, and the advantages of rewriteable media far outweigh the disadvantages.
- The process of copying fixed disks at BIOS level has enabled DIBS® to avoid problems with operating systems and access control mechanisms while the drive restoration process has proven capable of dealing with all currently available operating systems on the PC platform. In spite of these observations, no forensic copying system in current use offers equal protection to both the investigator and the computer owner. Note that this protection depends on neither how securely the copy cartridges are stored nor the relative security attending the storage of the floppy disks. Rather, it depends on the combination of all three and the technical security of the encryption mechanisms.
- When it comes to security readiness, company size doesn't matter. Larger companies (those with at least 1,000 employees) typically devote larger portions of their IT department's staff and budget to image verification and authentication security measures, but they are also more likely to have suffered security breaches, to have seen the number of security breaches increase from the previous year, and to have experienced more serious security problems.
- Security breaches normally cost larger companies $90,000, compared with $78,000 for smaller companies.
- Denial-of-service attacks are far more likely to occur at larger organizations.
- Larger companies are also more likely to be hit with a virus than smaller companies and more likely to have their Web sites defaced.

- CIOs who place a high priority on security will spend an average of $869,000 in 2005 on security measures and technologies; their counterparts who place a lower priority will spend an average of $654,000.
- The role of senior business executives in beefing up security is significant, but CIOs continue to express concerns about their executives' approaches to security.
- Indications are that CIOs often see their executives as paying lip service to aligning their companies' business practices with security concerns. At the same time, CIOs don't seem to be taking all the steps they could or should be taking to make security a higher priority for their companies.
- There aren't many significant differences between CIOs who assign a high priority to security and those who don't in terms of what security features they've put in place.
- Anti-virus software and firewalls are far and away the most frequently deployed technologies.
- Desktop anti-virus software is either already in place or in the process of being installed by the CIOs' companies.
- Technologies not yet widely deployed include image verification and authentication, decoy services, risk-assessment software, and public key information (PKI) document encryption.
- The only significant divergence between CIOs who view security as a high priority and those who do not is in the use of risk-assessment software, PKI document encryption, hybrid intrusion detection, and managed security services for firewall management.

An Agenda for Action

When completing the Computer Image Verification and Authentication Checklist (Table F8.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for computer image verification and authentication. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? There's a deficit of mathematical algorithms dealing with secure encryption, verification, and authentication of computer-based material.
2. True or False? It is not useful to present some fundamental requirements of a forensic data collection system before considering how these can be securely protected.
3. True or False? It must be understood that during the copying process, procedures are implemented to trap and handle hardware errors, mapping exceptions where necessary.
4. True or False? A digital ID (also known as a digital certificate) is a form of electronic credentials for the extranet.
5. True or False? The purpose of a digital ID is to reliably separate a public and private key pair with its owner.

Multiple Choice

1. Through Authenticode, the user is informed of the following, except for two:
   A. The true identity of the publisher
   B. A place to find out less about the control
   C. The authenticity of the preceding disinformation
   D. A place to find out more about the control
   E. The authenticity of the preceding information
2. As the Internet's leading certification authority, VeriSign has the following responsibilities, except:
   A. Publishing the criteria for granting, revoking, and managing certificates
   B. Granting certificates to applicants who meet the published criteria
   C. Managing certificates (enrolling, renewing, and revoking them)
   D. Storing VeriSign's root keys in an exceptionally unsecure manner
   E. Verifying evidence submitted by applicants
3. To save time, the Authenticode protocols use a cryptographic digest, which is a one-way hash of the document. The process is outlined by the following, except:
   A. Publisher obtains a software developer digital ID from VeriSign.
   B. Publisher creates unicode.
   C. Using the SIGNCODE.EXE utility.

D. The end user encounters the package.
E. The end user's browser examines the publisher's digital ID. Using the VeriSign root public key, which is already embedded in Authenticode-enabled applications, the end user's browser verifies the authenticity of the software developer digital ID (which is itself signed by the VeriSign root private key).

4. It is useful to present some fundamental requirements of a forensic data collection system before considering how these can be securely protected. These requirements were chosen to reflect the experience of computer forensic investigators. Other forensic experts may argue against some or all of them, except:
   A. Forensic data collection should be complete and non-software specific, thus avoiding software traps and hidden partitioning.
   B. In operation, it should be as slow and as difficult as possible to avoid error or delay.
   C. It should be possible for anyone to use a forensic data collection system with the minimum amount of training.
   D. Necessary costs and resources should be kept to a minimum.
   E. In operation, it should be as quick and as simple as possible to avoid error or delay.

5. Within the current raw data content of the suspect disk drive, a copy is also taken of the high section of conventional memory (to include any on-board ROM areas) and the CMOS contents via port access. This information is stored on each cartridge within a copy series. Also stored on each cartridge is a reference area containing copy-specific information such as the following, except:
   A. CPU type and speed; hardware equipment indicators
   B. Deleting drive serial number
   C. Cartridge sequence number
   D. Exhibit details and reference comments
   E. Operator name together with a unique password

Exercise

A company had contracted with a government agency to provide services for the agency's employees. The government agency alleged that the company had violated its agreement and filed a lawsuit. Discovery requests were onerous, to say the least; production of over two terabytes (2,000 gigabytes, the equivalent of 700,000,000 document pages) of data was mandated by the court. Almost all the data resided on backup tapes. It would be impossible for the company to meet this request using manual methods, and they lacked the internal technical expertise to produce the massive amounts of data involved in a cohesive electronic format. The company turned to a CFS team (CFST) to compile the data necessary to meet the discovery request. To narrow the scope of meaningful data, what did the CFST do?

HANDS-ON PROJECTS

An accounting firm was conducting an audit of a publicly owned company when they came upon some accounting irregularities. The irregularities were serious enough to potentially necessitate a re-stating of earnings. Considering the many scandals currently blighting the corporate sector, the accounting firm wished to confirm their findings before sounding any public alarms. They retained a CFST to conduct large-scale data mining to get to the bottom of the irregularities. How would a CFST go about conducting a forensics data mining operation?

Case Project

A bank suspected an employee of downloading sensitive files from the bank's computer network using his bank laptop computer from home while on leave of absence. The bank sent the computer to a CFST for computer forensic examination. What were the results of that examination?

Optional Team Case Project

A woman employed by a large defense contractor accused her supervisor of sexually harassing her. She was fired from her job for "poor performance" and subsequently sued her ex-boss and the former employer. A CFST was retained by the plaintiff's attorneys to investigate allegations of the former supervisor's harassing behavior. How did the CFST go about conducting the investigation?

REFERENCES

[1] "DIVA Computer Evidence: Digital Image Verification and Authentication," Computer Forensics UK Ltd, Third Floor, 9 North Street, Rugby, Warwickshire, CV21 2AB, U.K., 2002.

[2] "Software Publisher Digital IDs for Microsoft Authenticode Technology," VeriSign Worldwide Headquarters, 487 East Middlefield Road, Mountain

View, CA 94043 (VeriSign and other trademarks, service marks and logos are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries), 2002.

[3] "Vacca, John R., *Net Privacy: A Guide to Developing and Implementing an Ironclad E-Business Privacy Plan*, McGraw-Hill Professional, New York, 2001.

[4] "Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

Part III

Computer Forensics Analysis

The third part of this book covers the discovery of electronic evidence, identification of data, reconstructing past events, and networks.

This page intentionally left blank

9 Discovery of Electronic Evidence

Computer technology has revolutionized the way we deal with information and the way we run our businesses. Increasingly important business information is created, stored, and communicated electronically [1]. Many types of information that can play a useful role in litigation are no longer printed on paper and stored in paper files, but rather are stored in a computer system or in computer-readable form. As companies have increased their reliance on their computer systems, lawyers have begun to be aware of the valuable electronic treasures that are now being kept in these systems and have started aggressively to target electronic data for discovery in all types of litigation cases. The discoverability of these electronic files is referred to as discovery of electronic evidence or DEE.

Plaintiffs' lawyers have increasingly targeted electronic evidence for a number of reasons. It is also likely that electronic evidence will soon attract the attention of government investigators. Numerous statutory provisions empower government officials to enter, inspect, and make copies of records that must be maintained pursuant to various statutes and regulations.

The primary purpose of these provisions is to enable the government to determine whether a company is complying with the record keeping and other requirements contained in the statute that imposes them. Many businesses are increasingly storing the required records in electronic form. Government investigators will likely begin to focus their attention on the electronic forms of these records and the computer systems that house them.

The government also has access to records for investigatory purposes. Several statutes, such as the human rights codes, Competition Act, Criminal Code, and tax acts give government officials the right to enter a business establishment and inspect or seize records. For example, under the Competition Act, peace officers with, or in exigent circumstances without, a search warrant, may enter the premises, examine records, and copy or seize them. They may use the computer system on the premises to search data and produce printouts, which they may then seize for examination or copying.

Plaintiffs' lawyers and government investigators need to develop the knowledge and skills necessary to take advantage of the information residing in electronic form. This does not mean they need to become computer specialists, but rather, that they need to understand enough about technology to ask the right questions and enlist the assistance of the forensic computer experts where necessary. Lawyers who choose to ignore these new opportunities could expose themselves to malpractice claims.

Lawyers representing parties with large amounts of electronic data need to understand that their clients' data will be targeted for such discovery and need to advise their clients on how to prepare. Defensive strategies that should be implemented prior to litigation include a proper document retention program, periodic purging of magnetic media, and the implementation of a document management system. Once litigation has commenced, defendants need to be better advised on how to preserve relevant electronic evidence adequately—to avoid possible sanctions or a negative inference at trial.

Now, let's begin the discussion of electronic document discovery. This is the process of viewing log files, databases, and other data sources on unseized equipment to find and analyze information that may be of importance to a computer crime investigation.

ELECTRONIC DOCUMENT DISCOVERY: A POWERFUL NEW LITIGATION TOOL

Other than direct testimony by an eyewitness, documentary evidence is probably the most compelling form of evidence in criminal and civil cases. Often, important communications are committed to writing, and such writings can make or break a case. The same is true about documents used to conduct financial transactions. The *paper trail* has always provided a wealth of information in criminal and civil cases involving fraud. Traditional *paper* documents have been sought in the legal discovery process for hundreds of years in cases involving white collar crime (financial frauds, embezzlements). In more recent times, documentary evidence has become the keystone in civil cases involving wrongful employment dismissals, sexual discrimination, racial discrimination, stock fraud, and the theft of trade secrets. Today, judges and attorneys are very familiar with documentary evidence in paper form. Unfortunately, the legal process has not kept pace with computer technology, and the document discovery rules have changed concerning the discovery of computer-created documents and related electronic data.

In years past, documentary evidence was limited to paper documents. Subpoenas and court orders were issued for the production of specific documents, and the best evidence was typically considered to be the final draft of a document in paper form. Today, documents are rarely typed or handwritten. Most documents are created using personal computers with word processing applications or email programs. Most professionals rely on personal computers to maintain schedules and to create their written communications. Most computer users have become prolific writers because of the convenience that computers provide. As a result, more documentary evidence exists today than ever before and it exists in a variety of electronically stored formats. However, a majority of computer-created documents are never printed on paper. Many are exchanged over the Internet and are read on the computer screen. Thus, the legal document discovery process has drastically changed as it relates to computer-created documents.

The best evidence rules also work differently today, because copies of computer files are as good as the original electronic document. From a computer forensics standpoint, this can be proven mathematically. There is no difference between the original and an exact copy. In addition, modern technology has created new types of documentary evidence that previously did not exist. This is especially true for the creation of documents on a computer word processor. When electronic documents are created, bits and pieces of the drafts leading up to the creation of the final document are written in temporary computer files, the Windows swap file, and file slack. The computer user is usually not aware of this situation. Furthermore, when computer-created documents are updated or erased, remnants of the original version and drafts leading up to the creation of the original version remain behind on the computer hard disk drive. Most of this data is beyond the reach or knowledge of the computer user who created the data. As a result, these forms of *ambient data* can become a valuable source of documentary evidence. Lawyers are just beginning to understand the evidentiary value of computer-related evidence and computer forensics in the document discovery process. It is becoming more common for lawyers to seek production of entire computer hard disk drives, floppy diskettes, Zip disks, CD-ROMs, cell phones, and palm computer devices. These new forms of documentary evidence have broadened the potential for legal discovery.

Electronic document discovery is clearly changing the way lawyers and the courts do business when it comes to documents created with personal computers. From a computer forensics perspective, computer data is stored at multiple levels on computer storage media. Some levels are visible to the computer user and others are not. When computer files are deleted, the data is not really deleted. Fragments of various drafts of documents and email linger for months in bizarre storage locations on hard disk drives, floppy diskettes, and Zip disks. Government intelligence agencies have relied on these *secret* computer storage areas for years, but the word is starting to get out. Electronic document discovery is making a difference in civil and criminal litigation cases. This is especially true in cases involving the theft of corporate trade secrets and in wrongful dismissal lawsuits. The trail of computer evidence left behind on notebook and desktop computers can be compelling.

A historical perspective helps one understand the evolution of computer forensics and its transition into the new field of electronic document discovery. When computer mainframe giant International Business Machines (IBM) entered the personal computer market in October of 1981, the event quickly captured the attention of corporations and government agencies worldwide. Personal computers were no longer thought of as toys; almost overnight they were accepted as reliable business computers because of the IBM endorsement. Since their introduction, IBM PCs and compatible computers have evolved into powerful corporate network servers, desktop computers, and portable notebook computers. They have also migrated into millions of households, and their popularity exploded during the 1990s when people discovered the Internet.

The worldwide popularity of both personal computers and the Internet has been a mixed blessing. Powerful personal computers are technology workhorses that increase productivity and provide portability. The Internet provides a conduit for the transfer of communication and computer files anywhere in the world via personal computers. However, essentially all personal computers lack meaningful security. This is because security was not factored into the design of the original personal computers, or the Internet for that matter. The DOS operating system installed on the original IBM PC was never intended for commercial use. Security was never part of its design; in the interest of maintaining compatibility with the early versions of DOS, upgrades did not adequately address security. As a result, most popular desktop PCs and notebook computers lack adequate security. This situation creates an ideal environment for electronic document discovery of computer files, file fragments, and erased files. Some computer forensics specialists regard electronic document discovery as nothing more than the exploitation of the inherent security weaknesses in personal computers and the Internet.

You would think that the obvious security vulnerabilities of personal computers would be a wake-up call for government agencies and corporations. You would also think that individuals who carry *secrets* on their desktop and notebook computers would be more careful given these inherent security weaknesses. Lawyers, accountants, bankers, insurance agents, and health care professionals are particularly at risk because they are responsible for the *secrets* of others. It is likely that most lawyers don't even understand the potentials for attorney–client information to be compromised when computer files and data are exchanged with others. These security issues should be of concern to computer users. However, they provide great benefits to lawyers because of the potentials of electronic document discovery. Most computer users are unaware that their personal computers track their every move as it relates to documents created over time. This situation provides the technology savvy attorney with an edge when it comes to document discovery. Computer files, erased files, email, and ambient computer data can be subpoenaed in civil and criminal cases. The attorney just needs to understand the potentials and the new twist in thinking that is required to reap the benefits of electronic document discovery [2].

SUMMARY

Computers should now be considered a primary source of evidence in almost every legal case. With businesses and individuals relying on computers for data processing, scheduling, and communications, it is possible to discover anything from background information to the "smoking gun" document by investigating what is on your opponent's computer systems.

With that in mind, this chapter began with consideration of the process of information discovery. Because information discovery only deals with logical evidence (electronic data), you can avoid much of the tedium required by search and seizure to ensure evidence integrity and the chain of custody. Nevertheless, there are strong similarities between the two processes throughout their respective basic rules and planning stages.

Finally, for information discovery, where the basics are concerned, the investigator is occupied with safeguarding the chain of custody. During the planning stage, emphasis is given to understanding the information being sought. Backups of discovered information files are critical to the overall process, and tools such as revision-control software can be very handy for this task.

Conclusions

- With regards to the basics of the information discovery process, establishing and protecting the chain of custody for logical evidence should be straightforward.
- Three basic rules of thumb should act as guides for any information discovery. Each rule has a parallel in the world of physical search and seizure.
- The notable difference between searching for physical evidence and searching for logical evidence is that in the latter there is much less structure.
- Because the format and location of information varies tremendously from case to case, how information is discovered depends on the circumstances of the case and the imagination of the investigator.
- Once information is found, rigorous methods are applied to its handling and processing.
- Computer forensics may be applied: search and seizure and information discovery. Although different in their implementations, these areas share a few prominent common principals. These include the important concept that evidence should always be backed up and digitally authenticated prior to forensic

work. Both approaches require that everything the investigator does be carefully documented. In addition, for both areas, the evidence preservation lab plays an important role as a secure, controlled environment for computer forensics work and evidence storage. Without such a facility, the investigator will have a difficult (if not impossible) time maintaining the chain of custody while examining and holding evidence.

- The use of secure case-management software is highly desired because it lends structure, efficiency, and safety to the gathering and management of case notes and data.
- In a venue where law enforcement authorities are investigating a computer crime, there is a measurable chance that a case could find its way to court. Within a corporation or other organization, however, things are vastly different.
- Companies loathe being involved in litigation—even in situations where it appears the law is on their side.
- It's no surprise that legal fees and bad publicity can take a mighty toll on the "bottom line." For this reason, much of what the corporate computer fraud and abuse investigator does is for naught.
- It's easy for a corporate investigator to become frustrated and even disillusioned with his work when he sees good cases ending up on the wayside because of fears of bad P.R. Such feelings must be contained, as they will quickly result in laziness and incomplete work on the part of the investigator.
- Most of the computer crime cases handled by the corporate investigator won't end up in litigation.
- Even a seemingly low-profile case can take a sudden twist and end up garnering the attention of the CEO.
- Because practically any case can turn into a matter for litigation, the corporate investigator needs to treat all cases with a proper and reasonable amount of attention.

An Agenda for Action

When completing the Discovery of Electronic Evidence Checklist (Table F9.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for discovery of electronic evidence. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Other than direct testimony by an eyewitness, documentary evidence is probably the most compelling form of evidence in criminal and civil cases.
2. True or False? Biometric technology has revolutionized the way you deal with information and the way you run your businesses.
3. True or False? Numerous statutory provisions empower government officials to enter, inspect, and make copies of records that must be maintained pursuant to various statutes and regulations.
4. True or False? Many businesses are increasingly storing their required records in hard copy form.
5. True or False? CPAs representing parties with large amounts of electronic data need to understand that their clients' data will be targeted for such discovery and need to advise their clients on how to prepare.

Multiple Choice

1. Under the Competition Act, peace officers with, or in exigent circumstances without, a search warrant, may do the following, except:

   A. Enter the premises
   B. Examine records
   C. Copy records
   D. Seize records
   E. Delete records

2. In recent times, documentary evidence has become the keystone in civil cases involving the following, except:

   A. Wrongful employment dismissals
   B. Sexual discrimination
   C. Racial discrimination
   D. Stock options
   E. The theft of trade secrets

3. It is becoming more common for lawyers to seek production of the following, except:

   A. The entire computer hard disk drives

B. Land lines
C. Zip disks
D. CD-ROMs
E. Cell phones and palm computer devices

4. Since their introduction, IBM PCs and compatible computers have evolved into the following, except two:
   A. Weak mainframes
   B. Powerful calculators
   C. Powerful corporate network servers
   D. Desktop computers
   E. Portable notebook computers

5. As a result, most popular desktop PCs and notebook computers lack adequate security. This situation creates an ideal environment for electronic document discovery of the following, except:
   A. Computer files
   B. File fragments
   C. Added files
   D. Data miming
   E. Erased files

Exercise

A patient with a heart ailment was transported to a hospital where an angiogram was performed. The patient later had a stint inserted into an artery, along with a second angiogram, but died shortly thereafter. A third angiogram was performed immediately after the patient's death. Images of the angiogram procedures were purportedly stored on computer hard drives. The day following the patient's death, hospital staff were able to locate images for the first and third angiograms but could not find any images of the second procedure. The hospital and doctor were sued for medical malpractice and wrongful death. The plaintiffs also claimed the defendants had deliberately deleted the images of the second angiogram that allegedly proved the wrongful death claim. A CFS team (CFST) was engaged by the doctor's insurance company to locate images of the second angiogram on the computer hard drive. Explain the possible actions that the CFST took to locate the images.

HANDS-ON PROJECTS

The board of directors of a technical research company demoted the company's founder and chief executive officer. The executive, disgruntled because of his demotion, was later terminated; it was subsequently determined that the executive had planned to quit about the same time he was fired and establish a competitive company. Upon his termination, the executive took home two computers; he returned them to the company four days later, along with another company computer that he had previously used at home. Suspicious that critical information had been taken; the company's attorneys sent the computers to a CFST for examination. What did the CFST find during their examination?

Case Project

A CFST at a major financial institution in New York recently used a computer forensics tool to successfully preview two drives in Asia connected to the company-wide area network. The drives were previewed less than an hour after management determined that the investigation was necessary and that time was of the essence. The preview process revealed that one of the drives contained highly relevant information, and the drive was promptly acquired for further forensic analysis in New York [3]. What occurred during that analysis?

Optional Team Case Project

A large government agency, through a CFST, was able to enable a rapid incident response and capture sensitive data in a timely manner [3]. How was the CFST able to do this?

REFERENCES

[1] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

[2] "Electronic Evidence Discovery: A Powerful New Litigation Tool," New Technologies, Inc., 2075 NE Division St., Gresham, Oregon 97030, 2002.

[3] "EEE in Action: Real-World Scenarios" (Copyright 2004 Guidance Software, Inc.), Guidance Software, Inc., 215 N. Marengo Ave., 2nd Floor, Pasadena, CA 91101, 2004.

This page intentionally left blank

10 Identification of Data

The popularity of the Internet has grown at incredible rates and today it reaches into the hearts of many corporations and households worldwide. The Internet gives computer users access to a wealth of information. It is also a wonderful mechanism for the exchange of email communications and file attachments globally. International boundaries no longer exist when it comes to the exchange of information over the Internet. This new technology has proven to be ideal for international commerce and has the potential to be a valuable communications tool for exchange of law enforcement and government information. However, the Internet also provides the *crooks* with communication capabilities that did not exist previously. Through the use of a modem and with just a few clicks of a mouse, criminals can share information worldwide. It is sad but very true. Cyber crime has become a reality in our modern world.

More and more, law enforcement agencies are encountering computers at crime scenes. These computers are used to store the secrets of criminals and are used in the commission of crimes. Internet-related crimes are clearly on the rise, and abuses of corporate and government Internet accounts by employees are becoming commonplace. For example, one recent case involved an employee of a large corporation. He was using his corporate Internet account, on company time, to run his side business. What a deal—thanks to the Internet, he had two day jobs. To make matters worse, he was also using the corporate computers on company time to view and download pornographic images from the Internet. In another case, a law enforcement management official destroyed his 15-year law enforcement career when he was caught using a law enforcement computer to download pornography from the Internet. Just recently, law enforcement officials in Herndon, Virginia, requested help in the investigation of the rape of a young girl. The girl had been lured from an Internet chat room to meet the rapist at a shopping mall. When the rapist was finally caught, his computer contained crucial evidence in the case.

The law enforcement community is starting to effectively deal with computer-related criminal investigations. Funding is finally being focused on the creation of local and state computer crime units. Law enforcement training organizations such as the National White Collar Crime Center, Search Group, International Association of Computer Investigation Specialists, and the Federal Law Enforcement Training Center are training hundreds of law enforcement computer specialists each year. Some of these training efforts are directed at Internet-related crimes, and more training emphasis will be placed on this important technology issue in the future.

Let's look at how keeping an accurate and consistent sense of time is critical for many computer-forensic-related activities such as data identification. In other words, being able to investigate incidents that involve multiple computers is much easier when the timestamps on files (identified data) and in logs are in sync.

TIMEKEEPING

It seems that, although every computer has a clock, none of them appear to be synchronized—unless the computer in question is running the Network Time Protocol (NTP). With NTP, you can synchronize against truly accurate time sources such as the atomic clocks run by the National Institute of Standards and Technology (NIST), the U.S. Naval Observatory, or counterparts in other countries around the world.

NOTE

NTP is a protocol built on top of transmission control protocol/Internet protocol (TCP/IP) that ensures accurate local timekeeping with reference to radio, atomic, or other clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long periods of time. It is defined in STD 12, RFC 1119. The package that implements the latest version of NTP is called xntp™ and was developed at the University of Delaware. You can obtain the latest version of xntp via anonymous ftp to terminator.rs.itd.umich.edu in the file /unix/xntp/xntp-src.tar.Z. You may also find binary distributions there. Filenames for binary distributions will be named xntp-VERSION-OSNAME.tar.Z, (the binary distribution for SunOS is named xntp-3.4h-sunos4.tar.Z).

CAUTION

File names and URLs can change without notice.

What does accurate timekeeping have to do with computer forensics? Keeping a consistent sense of time is critical for many computer-forensic-related activities. Financial organizations rely on accurate timekeeping for their transactions. Many authentication systems, Kerberos being the most prominent example, use dated tickets to control access to systems and resources. Investigating incidents that involve multiple computers is much easier when the timestamps on files and in logs are in sync.

NTP began as a tool that permitted researchers to synchronize workstation clocks to within milliseconds or better. With the growth of the Internet, the mechanisms that enabled NTP clients and servers to securely exchange time data have gone from sufficiently secure to not nearly secure enough. Newer versions of NTP fixed the problem by providing a model for automatic configuration and key exchange. Let's take a look at time-synchronization systems, and how you can securely use them to set all your clocks accurately.

Time Matters

Why bother having accurate clocks? Isn't the one that comes in your desktop PC or your enterprise server adequate? The answer is that accurate timekeeping is an advanced science, an avocation practiced by hundreds of scientists around the world, and the paltry clock chip you have in your PC or expensive server winds up being a bit less accurate than your Swatch® watch for several reasons.

Computer clocks, like most electronic clocks, detect the oscillations of a quartz crystal and calculate the passing time based on these oscillations. Not all quartz crystals are the same to begin with, but put one inside a nice, hot computer that's cool whenever it's turned off, and the crystal's frequency tends to wander. Also, Unix systems base their notion of time on interrupts generated by the hardware clock. Delays in processing these interrupts cause Unix system clocks to lose time—slowly, but erratically. These small changes in timekeeping are what time scientists call *jitter*.

Over time, scientists and programmers have developed different techniques for synchronizing clocks over TCP/IP or other network protocols. The time protocol provides a server's notion of time in a machine-readable format, and there's also an Internet Control Message Protocol (ICMP) timestamp message. Though these remain available Internet standards, neither is currently sufficient for accurate timekeeping, and, hence, both are considered out-of-date. The Unix `r` commands include `rdate`, which permits setting a local clock based on a remote server. There are modem-based programs that contact NIST timeservers and fetch a time message (along with an estimate of round-trip time to account for latency), which you can still use today.

The NTP software includes drivers for a large number of devices—radios that listen to time signals such as WWV, global positioning system (GPS) receivers, and even atomic clocks—that serve as references for stratum-one servers. The University of Delaware site (*http://www.eecis.udel.edu/~mills/ntp/clock1a.html*) includes lists of stratum-one servers in the United States; you can also find stratum-one servers through Web search engines.

WWV is a radio station operated by NIST that maintains an atomic clock used by the scientific community.

Below stratum-one servers are many stratum-two servers; stratum-three servers are below that, and so on. NTP supports more than 15 stratums, but being closer to the top implies being closer to the most accurate source of time. To improve each server's notion of time, servers in the same stratum may peer (that is, act as equals) and perform the same timestamp exchanges done by NTP clients. NTP servers and clients don't blindly accept another system's notion of time, even if it comes from a higher stratum. This was NTP's only security provision for a while.

Clock Filters

Automatically accepting another system's statement about the current time can be harmful: suppose the timekeeping system has been taken over by an attacker who needs to *turn back the clock* so that a replay attack can function. NTP guards against this in several ways. First, NTP assumes that time moves forward, not backward, although small backward changes are acceptable. Also, if a system has been using NTP, the NTP software assumes that changes in a local clock will be small, generally less than a second. This makes controlling a local clock or making large changes literally a time-consuming process—even a one-second change is a big deal.

NTP goes beyond this by collecting timestamps from many servers (and peers, if appropriate). NTP maintains a queue composed generally of eight samples and uses carefully crafted algorithms to compute the best approximation of exact time. For example, the outlyers in the sample (the timestamps with the largest divergence) are discarded. The remaining set of samples is then used to calculate what the local clock should read. On Unix systems, a special system call, `adjtime ()`, makes small adjustments to system time. With multiple sources, the influence of a single, compromised timeserver (a falseticker, in NTP jargon) is completely avoided. You can modify the configuration of ntpd to label a timeserver as untrusted. You can also use the configuration to list trusted timeservers and peers.

By the late 1980s, version 2 had been released. NTP 2 included digital signatures based on a shared secret key so that servers and peers could sign NTP data and prevent an attacker from spoofing packets. NTP uses user datagram protocol

(UDP) packets (on port 123), which are easy to spoof because of their stateless nature (no connection setup, as in TCP).

Autokey

Version 4 of NTP has now entered the internet engineering task force (IETF) standards track. The most interesting aspects of version 4 are the security improvements. A system called the autokey uses public key algorithms combined with a list of one-way hashes. When a client contacts an NTP server, the client can collect a certificate that contains the server's public key and independently verifies it. Then, using the enclosed public key, the client can check the signature sent by the server containing a list of key ids. The key ids are used with session keys to perform a quick digital signature check based on Message Digest 5 (MD5).

Using public key cryptography for signing timestamps is just too slow. Public key encryption algorithms aren't only slow (compared to private key algorithms such as RC4), they're also inconsistent in that the amount of time used to encrypt may vary by a factor of two—something very unpleasant for those obsessed with keeping accurate time. Using the list of key ids reduces the need for public key encryption to once an hour on average.

Version 4 also supports the Diffie-Hellman key exchange for peers, so that peers can exchange private session keys. Multicast updates of clients are also supported and use the client/server autokey for setting up security.

FORENSIC IDENTIFICATION AND ANALYSIS OF TECHNICAL SURVEILLANCE DEVICES

It was one sentence among hundreds in a transcription of a dull congressional hearing on the environment, a statement anyone might have missed: Bristol-Myers Squibb Co. was looking to increase its harvest of the Pacific yew, a protected tree. However, the competitive intelligence (CI) officer at arch rival SmithKline Beecham Corp., happened to catch it, thanks to a routine search of competitors' activities on the Web.

The intelligence officer sprang into action. He knew Bristol-Myers' researchers had been testing a substance in the tree's bark as an experimental agent against breast cancer. But why was Bristol-Myers suddenly seeking to cut down 200 times as many yews? Was it ready to put its planned anticancer drug, Taxol, into production? Back at SmithKline headquarters in Philadelphia, the news was enough to trigger serious nail-biting in the boardroom. SmithKline was developing its own anticancer drug, Hycamtin, but it wouldn't be ready for another 18 months. Would it beat Bristol-Myers' drug to market? Or would SmithKline Beecham have to speed up its production schedule—and if so, by how much?

The intelligence officer's team wasted no time. It immediately began canvassing conferences and scouring online resources for clues. It tapped into Web sources on the environment and got staffers to work the phones, gathering names of researchers working for Bristol-Myers. It even zeroed in on cities where Bristol-Myers had sponsored experimental trials of the substance.

Sure enough, Bristol-Myers had been taking out recruitment ads in those areas' newspapers for cancer researchers—a sure sign that Bristol-Myers was stepping up its hiring of oncologists specializing in breast cancer. The next clue? From data discovered on financial Web sites and in the comments of Wall Street analysts, the intelligence officer's team discovered that Bristol-Myers was increasing its spending on its oncology group.

That was all the intelligence officer needed to hear. Senior R&D managers were ordered to speed things up and ended up rushing Hycamtin to market in 6 months instead of 18—preserving SmithKline some $50 million in market share and millions in drug development costs. The CIA, the National Security Agency, and England's MI5 used a form of CI to figure out what the Russians were doing. SmithKline used it too.

SmithKline Beecham's tale of how competitive intelligence saved a company millions is no longer unusual. Indeed, one of corporate America's worst-kept secrets these days is that more and more companies, from Burger King to Nutrasweet to MCI, are spying—and have in-house operations to keep tabs on rivals. The number of large corporations with CI units has quadrupled since 1997, and spending on CI is estimated to be around $32 billion annually—nearly double the amount spent just two years ago.

To be sure, data-diving isn't new. As far back as the 1970s, in a now-famous example of excess zeal, The Boeing Company discovered that a Russian delegation visiting one of its manufacturing plants was wearing crepe-soled shoes that would surreptitiously pick up metal shavings off the factory floor to determine the type of exotic metal alloys Boeing was using in its planes. And at Motorola Inc., the former chief of CI used to work for the CIA.

Now, thanks to the Net and its ever-growing, low-cost reach and speed, nearly everybody's spying. In a May 2003 survey by marketing firm TR Cutler, Inc. (*http://www.trcutler.com/*), 77% of U.S. manufacturing companies with fewer than 3,000 employees admitted to spying on competitors during the previous 12 months, using the Web and posing as potential customers to glean pricing and other competitive tidbits.

Corporate Information

Now, here's a real secret: until recently, most corporate gumshoeing was being outsourced to spy companies with 007-sounding names such as WarRoom Research

Inc., many of which were founded by ex-CIA, National Security Agency, and Mossad operatives seeking work after the Cold War. Now, though, corporate snooping is increasingly being conducted in-house—and for the first time, chief information officers (CIOs) are being forced to the frontlines. More and more CIOs are gaining responsibility for the intelligence function. And why not? Information is about technology, and information is increasingly a company's competitive edge.

To be sure, companies without the ability to pluck the juiciest scoops from a growing quagmire of data will increasingly lose market share to those companies that can. This is now a double-edged sword. Those who get spied on are now also spying. Case in point: The CIO of 3COM Corp. (*http://www.3com.com/selectsite.html/*), makers of Internet switches and hubs, now supplies employees with two toll-free numbers: one to report any intrusions into corporate secrets, the other to report what 3COM's rivals are up to. You've got to take the offensive these days or you'll be clobbered in the marketplace, and the spy-versus-spy mentality is only being exacerbated by the stiffening competitive pressures of the current economy.

What is CI? Everything from illegal spying and theft of trade secrets to classic intelligence-gathering—whatever it takes to provide executives with a systematic way to collect and analyze public information about rivals and use it to guide strategy. At its best, CI borrows tools and methods from strategic planning, which takes a broad view of the market and how a company hopes to position itself, and from market research, which pinpoints customers' desires. Its goal: to anticipate, with razor-sharp accuracy and speed, a rival's next move, plot new opportunities, and help avert disasters.

CI is hottest in the pharmaceuticals, telecom, petrochemicals, and consumer products industries, where consumers are the most fickle and where speed and flexibility are especially critical for success. Indeed, some companies, from Burger King to Lucent Technologies Inc., are getting so good at using the new digital tools to sniff out what rivals' customers are eating this week or paying for long-distance that it's enough to rattle even the most rival-savvy marketers—and to push a lot of data, once commonly available, underground.

For example, in 2002, Wal-Mart Stores Inc. ended a years-long practice of sharing data about its sales of food, beverages, toys, clothing, and over-the-counter medications. Gathered by electronic scanners in checkout aisles, the data had been closely monitored by various parties—from the companies that make products sold in Wal-Mart's more than 4,800 stores to Wall Street analysts.

Competing at the speed of information can pay off handsomely. NutraSweet estimates its intelligence unit is worth at least $70 million a year in sales gained or revenues not lost. SmithKline Beecham estimates saving more than $300 million and gaining untold protection of market share for any number of products. All information is now being thrown into the digital hopper and sliced and diced for clues and leaks. It's a CIO's gold mine.

What is the real bottom line? The new business-led push to get better competitive data (faster) is also defining new opportunities for CIO leadership at most firms. The CIO who is just responsible for wires, equipment, and software now knows about hacking and penetration. Those responsible for business intelligence activities will really be clued in; companies who have CIOs with competitive leadership abilities, will have the competitive edge in the years ahead.

Information Overload

The growing information glut makes it critical for CIOs to start thinking about how they can support their company's CI snoopsters—and do it with as much zeal and imagination as they already apply to building hacker-proof security systems. Most existing systems and organizations are still ill-equipped to keep pace with the ever-growing amount of information available. Many companies are still stumbling to process and respond to competitive information as fast as it pours in. The result is that the key to carving out the leading edge of the knowledge gap in one's industry (the difference between what you know and what your rival knows) lies in the ability to build IT systems that can scope out the movements of corporate rivals in real time. IT-aided intelligence gathering is so critical that entire industries will be redefined by the companies most skilled at snooping. Players unable to surmount their bureaucratic inertia will find their existence threatened. Once intellectual and competitive agility becomes more commonplace, competitive advantage will be both harder to come by and increasingly expensive.

Therefore, it is recommended that you now start recruiting the technology executives who can build systems that will give your company the ability to react in real time to what its rivals are doing. Build such systems, and your company also will be able to respond faster to customers. The goal is to tie technology and business together in a common pursuit of becoming more competitive and responsive to rivals and customers in the marketplace. CI is to a company what radar is to an airplane. Companies are now installing radar in the corporate cockpit, and that's where the CIO comes in.

At minimum, CIOs should start helping executives monitor the Web more effectively. The Net is opening up whole new ways to snoop, giving companies access to material that used to take months or years and millions of dollars to unearth, from satellite photos of rival plant sites, to the inside skinny on a rival CEO's off-work activities. And it's legal. For example, the London-based consumer products firm Unilever plc was looking to go into China with a new product, but Dollens and Associates' (Chicago-based) chief technology officer (CTO), by going on the Web, discovered that Proctor & Gamble was developing a similar product. Unilever, the CTO's client, had to decide whether to offer that product at a lower price, add on more features, or simply avoid the Chinese market entirely. How did Unilever get wind of P&G's plans? The CTO found P&G's new product report on P&G's own corporate intranet—access to which Unilever was able to get through the CTO and a common supplier. Without this information, Unilever would have gone into China blind.

It takes far more than watching Web sites to get smart about CI. At Royal Dutch/Shell Group, the CIO is part of the CI team and is in charge of helping corporate snoopers gather and distribute key bits of information about rivals to company executives. Shell's CI office provides the CIO with benchmarks on competitors, and the CIO then develops customized search software to help the CI team sift through files. At Shell, the CI is all about aiding the decision-making process. It's a mix of technology and people. Ideally, the CIO should be the hub for CI throughout the company.

Most CIOs are still far more likely to shop for technology than actively participate in CI tag teams and strategy sessions, but increasingly, companies like P&G are realizing they cannot move forward on CI without asking CIOs to help tag and distribute priority data to the people inside the company who most need to know.

Companies that ignore the CIO do so at their peril. Recently, that happened to a large telecom equipment maker with 30,000 home pages on its supply-chain intranet. Several hundred of the home pages were dedicated to the competition, but there was no coordination between home pages. This was a situation where the CIO could have taken charge and made sure the information was in one spot. How many tens of millions of dollars were thrown at that intranet and wasted annually in inefficient man-hours?

Ideally, CIOs can help marketing and sales strategies turn on a dime. CI teams should spend one-third of their time gathering information on a project, one-third in analysis, and one-third discussing their findings. Instead, many companies spend 80% of their CI time on collection, most of the rest on analysis, and very little on communication that reaches everyone. CIOs can step in and devise ways to improve the ability of executives to focus on information that really matters to them, with filters that take out the junk nobody needs to be looking at.

CIOs also can help determine what the company considers junk. Often the best competitive information does not appear as highly structured data, such as financial information. More likely, it's something like an offhand comment in a press release, a photograph in a rival's advertisement, or a soundbite from a television news show.

Once the best data is tagged for collection, who gets access to it? If you search for data involving a two-in-one laundry soap and fabric softener, what terms do you classify, and what do you let everyone see? CIOs can help companies figure out how to tag, gather, store, and distribute a wide range of competitive data with differing levels of access and indexing—and with standards that are consistent throughout the company, domestically and abroad. Most companies are sloppy about this. They haven't marked documents as confidential, and nobody beyond a certain level knows what specifically they're looking for. They just know they want something, and fast. With a proliferation of business relationships these days (joint ventures, supply-chain collaborations, and so forth) you really need to do an information audit to make sure you know what you have and what you need.

Building Teams

You need to build teams with diverse membership. People who understand the concept of organizing information and indexing it could be paired with someone who understands different technology capabilities, such as a relational database showing connections between different terms or items. As managers, CIOs have to amass different strengths on a CI project *so they don't have an abundance of hammer holders who look only for nails.*

However, don't get carried away on the technology. A few years ago, a study conducted by Fuld & Company [1] found flaws with many of the 170 software packages with potential CI applications. None of them were able to take companies through the process of data identification, discovery, distribution, and analysis. Each did some part of the process, but not the whole thing. The thinking machine has not yet arrived. No company should buy a software package in the hope it will build an intelligence process for the corporation. CIOs need to help build that. It won't come off the shelf.

Still not convinced? CIOs confident that their rivals' intranet data is too safe to even try prying open should take a ride (fly or drive) down Virginia's Dulles Corridor, a throughway outside Washington, DC that is lined with high-tech firms. If you have a laptop, slip a wireless card [2] into it and drive down Route 7 or fly around Northern Virginia. You can actually pick up one wireless network after another (hot spots), including the networks of a major credit clearinghouse and Department of Defense contractors that store classified data on their servers. Instead of hacking from the Internet, people can hack from inside on the intranet (known as war flying or war driving), albeit from the road or by air, and probably get to the accounting server or worse. Imagine the kind of damage a terrorist organization could do.

NOTE

War driving or flying is the activity of driving around in a car or flying a plane around for the purpose of searching and pinpointing the location of wireless networks or hot spots in metropolitan areas. Recent surveys have revealed that 80% of these hot spots are not protected by firewalls, encryption, or intrusion detection systems.

For all the digital dumpster-diving out there, don't forget that plenty of old-fashioned snooping is still being used by even the most high-tech firms. For example, when Oracle Corp. got caught (in the summer of 2000) hiring a Washington, DC–based detective group to dig into the dealings of organizations sympathetic to Microsoft Corp., it didn't use even a byte of cyber sleuthing. It did it the old-fashioned way—rummaging through the dumpsters of one of those groups by bribing janitors at its Washington office.

In other words, in this business, you need to be aggressive. Take the offensive. Always recall the words of ancient Chinese general Sun Tzu (6th–5th century B.C.): "Be so subtle that you are invisible, be so mysterious that you are intangible; then you will control your rival's fate."

SUMMARY

As previously explained, computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored in the form of magnetically encoded information (data) [3]. Many times the computer evidence was created transparently by the computer's operating system and without the knowledge of the computer operator. Such information may actually be hidden from view and, thus, special forensic software tools and techniques are required to preserve, identify, extract, and document the related computer evidence. It is this information that benefits law enforcement and military agencies in intelligence gathering and in the conduct of investigations.

Computer forensic software tools and methods can be used to identify passwords, computer network logons, and other information that is transparently and automatically transferred from the computer's memory to floppy diskettes, Iomega Zip Disks, and computer hard disk drives. Such computer forensic software tools and methods can also be used to identify backdated files and to tie a floppy diskette to a specific computer.

Trade secret information and other sensitive data can easily be secreted using any number of techniques. It is possible to hide diskettes within diskettes and to hide entire computer hard disk drive partitions.

The last section of this chapter discussed a deterrence-based approach as an element of an overall cyber defense strategy. The need for timely and unequivocal identification of attackers is essential for such an approach to be effective. Unfortunately, the technical basis for such identification has not received much attention from the research and development community. In addition, there may be some complicating factors for the implementation of the type of identification and forensics capability discussed in this chapter, such as the widespread move to encryption. However, until research and development resources are committed to investigation of the relevant issues, the extent of the challenge cannot be fully understood.

Conclusions

- The hiding of data in computer graphic files (steganography)
- Detection of steganography and watermarks
- Steganography jamming techniques and theory
- Data written to “extra” tracks
- Data written to “extra” sectors
- Data written to hidden partitions
- Data stored as unallocated space
- Massive amounts of data written to file slack areas
- Data hidden by diffusion into binary objects, Windows swap, and Windows page files
- Hidden disks within disks
- Floppy diskette data storage anomaly detection
- Data scrubbing of ambient data storage areas. These security processes are especially helpful when computers are transferred from one user to another.
- Data scrubbing of entire storage devices using methods that meet current Department of Defense security requirements
- The potential risk of shadow data issues
- The appending of data to program files, graphics files, and compressed data files—simple and very effective
- Electronic eavesdropping techniques, threats, risks, and remedies
- Covert capture of keystrokes via hardware and radio interception
- Tempest issues regarding the remote capture of computer screen images
- Electronic eavesdropping techniques concerning cellular telephones
- Electronic eavesdropping techniques concerning personal pagers
- Search methodologies for use in the identification of foreign language phrases in binary form stored on computer media

An Agenda for Action

When completing the Identification of Data Checklist (Table F10.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for identification of data. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let’s move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? It seems that, although every computer has a clock, none of them appear to be synchronized—unless the computer in question is running the Network Time Protocol (NTP).
2. True or False? Data-diving isn't new.
3. True or False? Deterrence is a fundamental element of defensive strategy.
4. True or False? Computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored in the form of magnetically encoded information (data).
5. True or False? Computer forensic software tools and methods can be used to identify passwords, computer network logons, and other information that is transparently and automatically transferred from the computer's memory to floppy diskettes, Iomega Zip Disks, and computer hard disk drives.

Multiple Choice

1. Law enforcement training organizations such as the following (except for one) are training hundreds of law enforcement computer specialists each year.

   A. NRA
   B. National White Collar Crime Center
   C. Search Group
   D. International Association of Computer Investigation Specialists
   E. Federal Law Enforcement Training Center

2. The NTP software includes drivers for a large number of devices, except for two of the following that do not serve as references for stratum-one servers:

   A. Radio telescopes
   B. Land lines
   C. Radios that listen to time signals such as WWV
   D. Global positioning system (GPS) receivers
   E. Atomic clocks

3. The CI's goal is to do, with razor-sharp accuracy and speed, the following, except for two:

   A. Anticipate a rival's next move
   B. Plot new opportunities

C. Help avert disasters
D. Help cause disasters
E. Plot new attacks

4. Which one of the following do financial organizations rely on for the accuracy of their transactions?

A. Computer files
B. File fragments
C. Timekeeping.
D. Data miming
E. Erased files

5. Which one of the following began as a tool that permitted researchers to synchronize workstation clocks to within milliseconds or better?

A. NTP
B. TCP/IP
C. DOS
D. BIOS
E. WEP

Exercise

A CFS team (CFST) arrived at a company site to collect computer evidence from a server. The company was not the perpetrator of the investigated crime but apparently did possess imported evidence that resided on a mission-critical server that could not be taken offline [4]. What did the CFST do to collect key evidence to solve this problem?

HANDS-ON PROJECTS

The CTO of a large beverage company suspected something was amiss when he noticed a significant amount of traffic traveling through the company network. He deduced that his trusted staff of system administrators might have been misusing their access privileges and the network servers for some unknown purpose. A CFST was contracted to perform a confidential after-hours investigation of the network and the system administrators [4]. What did they find out?

Case Project

A large multinational corporation was accused of questionable financial reporting by the SEC, resulting in an investigation by a major independent consulting company. The goal of the investigation was to determine if the chief financial officer had ordered his staff to alter or destroy transactions to help the company's financial position appear more favorable [5]. How did the CFST go about performing an exhaustive search of all computer records within the company's large finance division?

Optional Team Case Project

A public institution was the victim of a hacker. The subject got into the network and placed several large media files on several computers and changed the desktop configurations. Management decided against calling law enforcement initially (because of media attention) and instructed the IT department to get a CFST to privately investigate. The IT department called and the CFST consulted on the case [5]. How did the CFST go about doing this?

REFERENCES

[1] Fuld & Company Inc., 126 Charles Street, Cambridge, MA 02141, 2002.

[2] Vacca, John R., *Wireless Broadband Networks Handbook: 3G, LMDS and Wireless Internet*, McGraw-Hill Professional, New York, 2001.

[3] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

[4] "EEE in Action: Real-World Scenarios" (Copyright 2004 Guidance Software, Inc., Guidance Software, Inc.), Guidance Software, 215 N. Marengo Ave., 2nd Floor, Pasadena, CA 91101, 2004.

[5] Mandall, Robert, Computer, Forensic Evidence Solutions, Inc., (© 2002 Computer Forensic Evidence Solutions, Inc.) 1212 Hope Ranch Lane, Las Vegas, NV, 2002.

This page intentionally left blank

11 Reconstructing Past Events

The increase in computer-related crime has led to the development of special tools to recover and analyze computer data. A combination of hardware and software tools has been developed using commercial off-the-shelf utilities integrated with newly developed programs. Procedures have been defined and implemented to protect the original computer data. Processes have been developed to recover hidden, erased, and password-protected data. To that end, all recovery and analysis work is performed on image copies of the original.

Because there is a wide variety of computers, peripherals, and software available, including many different forms of archival storage (Zip, Jaz, disk, tape, CD-ROM, etc.) [1] it is important that a wide variety of equipment be available for recovery and analysis of evidence residing on a computer's hard disk and external storage media. Recovered data must be analyzed, and a coherent file must be *reconstructed* using advanced search programs specifically developed for this work.

For example, these techniques were recently used to recover data from several computers that indicated a large check forgery ring was in operation throughout California and personal and business identities were being stolen without the knowledge of the victims. Case files going back over five years were cleared with the information obtained.

In another case, proprietary intellectual property was found on the suspect's computer and was being used for extortion. In the case of a murdered model, the murderer's computer address book was recovered and is now being used to determine if he might be a serial killer. Another case involved a stalker who had restricted pager information on his victim, which was recovered from the suspect's computer.

The primary goal of this chapter is to illustrate how to reconstruct past events with as little distortion or bias as possible. Many analogies can be drawn from the physical to the virtual realms of detective work. Anyone who has seen a slaying on a police show can probably give a reasonably good account of the initial steps in an investigation. First, you might protect and isolate the crime scene from outside disturbances. Next, comes recording the area via photographs and note taking. Finally, a search is conducted to collect and package any evidence found.

HOW TO BECOME A DIGITAL DETECTIVE

Recovering electronic data is only the beginning. Once you recover it, you need to determine how to use it in your case. In other words, how do you reconstruct past events to ensure that your findings will be admissible as evidence in your case? What follows are some recommendations for accomplishing that goal.

If You Need Help, Get Help

When you receive the package of evidence containing a Zip disk and cover letter stating, "Enclosed and produced upon your request, please find ...," you may not know what to do with the disk. If you don't know, get help.

Help may be just down the hall. If you have an information services department, consider going there. They might not understand what you mean by a discovery request, but they may be able to help you convert the contents of the disk to a form you can look at. If you have a litigation support group, consider contacting them. They may have the tools you need to look at and start working with the data you just received. Even if there is no formal entity within your office dedicated to dealing with technological issues, there may be informal resources.

In addition, your client may have the resources you need. Your expert witnesses, assuming you have some, may be able to sort out the data for you. If you are using a litigation support vendor, that organization may be able to bring skills to bear. Of course, don't forget the professionals, the ones who deal with electronic data recovery and reconstructing past events for a living.

Convert Digital Evidence

Before you can reconstruct past events and present the data, you need it on a medium and in a format you can work with. In other words, you need to get the data onto a medium you can use, if it is not already on one. Today, data can come on a variety of media, such as holograms, video, data tapes, Zip disks, CD-ROM disks, and even 3.5-inch floppy disks.

If you receive electronic evidence on an 8-mm data tape, chances are that you will not have an 8-mm tape drive at your desk. Even if you have a drive, it may not be able to read that specific tape. You need to get the data onto a medium your computer can read, which these days generally means a 3.5-inch floppy or a CD disk. How do you do this?

For example, you could use Zip disks. Zip disks are simpler. The cost of Iomega Zip drives (*http://www.iomega.com/global/index.jsp*) is so low that you can keep one on hand just to copy data from Zip disks you receive (and to copy data to Zip disks when others request data from you on that medium). CDs are even simpler, as CD drives have become commonplace on PCs. Similarly, even 3.5-inch disks generally pose no problem.

Put the Evidence in a Useable Format

Having data on a useable medium is useless unless it also is in a useable format. At times this is not an issue. If the data comes in a format that you already use, then you can begin to work with it as soon as you get it off the media. The formats most likely to be useable without conversion are word processing files (principally WordPerfect and Word files), spreadsheet files (principally Excel and Lotus), and presentation files (principally PowerPoint files).

USEABLE FILE FORMATS

Even if the data is in a format that appears to be one you already use, conversion still may be necessary. The format may be too new. The problem is a basic one. In a similar vein, you may have to get the data converted if it comes to you in a format that is too old or runs on a different operating system. Although simple files created with one company's software generally can be opened without a problem using a competitor's comparable product, this often does not hold true for more complex files.

UNUSABLE FILE FORMATS

You may get electronic data in a format that you cannot use "out of the box." When that happens, you have to convert the files to a format you can use—or find someone to do the conversion for you. You may have already encountered these issues with a variety of files including email files, database files from mainframe systems, and ".txt" files containing data dumped from database files. Anyone who has undertaken this task can attest that it is potentially a difficult and painstaking process.

Whenever you suspect that you will have to convert data, there are some steps you can take to facilitate the process. Initially, try to get as much information about how the files were created and maintained as you can. Whether you intend to try the conversion yourself or rely on outside resources to get the work done, the more you know about the files, the better your chances of a successful conversion. For example, if you receive a ".txt" file that appears to contain information from a database file, try to find out, among other things, the make and model of the computer the file came from; the name and version of the operating system the computer ran; the name and version of the database program used; the name of the database file; a list of all fields in the database; and descriptions of each field with the descriptions including the type, length, and other characteristics of the field.

Furthermore, get sample printouts if possible. If you get these, they may provide answers to some of the questions previously listed. They may show how the data was laid out—and, hence, how it was used. They also may give clues about electronic data that you should have received but did not.

CONVERTING FILES

If you are going to attempt converting the data yourself, you may be fortunate enough to have received electronic data that you can covert directly into programs such as Access or Excel using the wizards built into those programs. This can be the case with ".txt" files. Sometimes the first line in a file you are converting may even contain the names of the fields that need to be created, further simplifying your task. If that information is not in the file, then try to get the field names and descriptions from the producing party. Should you fail at that, you may have an exceedingly difficult time carrying out a meaningful conversion.

Sometimes data will not be in a format amenable to immediate conversion. Email files are a common example.

Get the Right Software, Hardware, and Personnel

Concomitant with getting the data into a useable format is getting the right software, hardware, and personnel to work with the format you choose. For software, you may have already found that Access, Excel, and Concordance (*http://www.mario.uklinux.net/concordance/*) meet most of your needs, but there are, of course, a plethora of other good tools available.

NOTE

Concordance is a program that scans a text file and outputs concordance lines based on a node entered by the user.

Hardware requirements will vary greatly depending on specific circumstances. For example, 100 kb of data can be handled by any machine and across any network. A hundred gigabytes of data still pose very few problems. However, 100 terabytes of data does pose some substantial challenges in terms of hard drive space, backups, network traffic, and, for that matter, performance. When faced with data of that quantity, you need to set up dedicated machines that do not pass queries or results across your network.

Personnel requirements present the greatest challenge. If you are going to make sense of the electronic data you have received, converted, and loaded, you need know how to use the tools yourself, or, failing that, rely on someone who can use the tools for you. As previously discussed, you may already have the personnel you need in your own office or you may have to turn to outside resources. Also, once you are in a position to work with the electronic data you got from outside resources, check that the data is what it ought to be.

Did You Get All the Data?

Check to see whether you received all the data you should have received. Prepare an inventory of what you received and compare it against what you requested. This may be as simple as preparing and comparing lists of file names. More likely, however, it will require that you develop short descriptions of the data you received and then match the descriptions with your discovery requests. It may even mean you will have to closely analyze the data to see whether gaps emerge that indicate some failure to produce all that it ought to have produced.

You also can search the electronic data for references to electronic files that should have been given to you but were not. This can be done through a manual review. The manual review can be enhanced if the software you are using to review the data allows you to search for strings of characters. If it does, you can search for filename extensions that are typically associated with the types of files you want to find. Examples include .doc, .htm, .html, .htx, .rtf, .mcw, .txt, .wps, and .wpd for word processing files; .csv, .dbf, .dif, .txt, .wk1, .wk3, .wk4, .wks, .wq1, .xls, and .xlw for spreadsheet files; and .asc, .csv, .dbe, .dbf, .htm, .html, .mda, .mdb, .mde, .mdw, .tab, .txt, and .xls for database files.

If you received spreadsheet or database files in their native format, you can scrutinize them for signs of links to files that were used in connection with the files you got but that were not given to you. In a spreadsheet file such as an Excel file, this might mean searching the cells for extensions such as the ones previously listed. It also can mean checking the “properties.” If you are asked whether you want to reestablish a link when you open the file, that is a clear sign of potentially missing files; keep track of the file names and check to see whether you received them. In a database file such as an Access file, this means closely examining all tables, queries, forms, reports, macros, and modules for references to other files.

Did the Evidence Come from the People You Thought It Would?

Files often contain indications of who created them, who worked on them, and who last saved them. If you go to File | Properties, you can sometimes find this information.

Look for "Hidden" Data

Electronic files often contain "hidden" data (information that does not show up on any printouts of the file) that can potentially prove useful. You should go to File | Properties, where you may be able to find out a host of details about the file that the people sending it to you may never have known went with it. These can include when the file was created; when it was last modified; who created it; what comments have been added; what title was given to the file; whether intentionally or automatically, which subjects have been assigned to the file; who last saved the file; and how many revisions the file has gone through.

In word processing files, look for comments that display on the screen, but do not automatically print out. If there are tables containing numbers, check them for a formula that calculates the figures displayed in the tables. If there are objects embedded in the word processing file, such as portions of spreadsheet files, try to ascertain the names of source files.

In spreadsheet files, look at the formula; these show the true work being done by the spreadsheet file in a way that a printout never can. Check the formula for references to other files. Look for hidden columns. If the column listing across the top reads "A B C E H," that means there are at least three hidden columns (D, F, and G) that might contain information of greater value than anything shown. Watch for comments; in Excel, these may initially only show up as small red triangles at the upper right corners of cells. Beware of cells that appear to be empty but are not.

In database files, look for an explanation of field names or contents; in Access, you might find this by looking at the database tables in "design" mode. Look for links to files you did not receive; in Access, this might be indicated by small arrows to the left of the table icons. Look for tables, queries, forms, reports, macros, and modules that you did not know about. In tables, look for hidden fields.

Test the Data

Test the electronic data to determine how complete, accurate, and reliable it is. You can test the data against itself. Look for inconsistencies. Look for errors as well.

Where feasible, the electronic data can be compared to underlying documents, again to determine the completeness, accuracy, and reliability of the data. This comparison can highlight coding errors made when creating the database such as wrong numbers, dates, and names. It also can reveal categories of information that were not added to the electronic data, which if they had been added, would have affected the results of searching the data. Just as electronic data can be compared to underlying documents, so also can it be compared to data in other electronic files, the contents of other documents, and information available through the Internet.

Work the Evidence

What one can do with data really is limited more by one's imagination than anything else. That said, there are several general recommendations that can be offered: Put the data into tools you can use. Spreadsheet programs can allow one to perform calculations, prepare pivot tables that can quickly summarize data across several dimensions, develop charts to graphically present trends in the data, and map out information geographically. Database programs can permit one to search or query the databases in complex and subtle ways, perform calculations, and generate a broad range of reports. Sharing the data you receive and the knowledge you glean from it to reconstruct past events with your client, experts, and other colleagues, as appropriate, can offer you the opportunity to more effectively handle your case.

SUMMARY

Once the data has been successfully collected, it must be analyzed to extract the evidence you wish to present and to rebuild what actually happened. As always, you must make sure you fully document everything you do; your work will be questioned and you must be able to show that your results are consistently obtainable from the procedures you performed.

Finally, this is where logging utilities come in. Logging utilities are vital for forensics when reconstructing the sequence of events leading up to, during, and after an attack, provided the attacker doesn't delete the log files. Refining the firewall rules, keeping the intrusion detection systems (IDSs) current, and reviewing the log files will be important to stay one step ahead of the bad guys.

Conclusions

- Computer forensics is the principle of reconstructing the activities leading to an event and determining the answers to "What did they do?" and "How did they do it?"
- Stored information can be volatile and persistent at the same time.
- Collecting electronic evidence is no trivial matter. There are many complexities you must consider, and you must always be able to justify your actions.
- Gathering electronic evidence is far from impossible. The right tools and knowledge of how everything works is all you need to gather the evidence required.
- Audit trails can also be used to reconstruct events after a problem has occurred.

An Agenda for Action

When completing the Reconstructing Past Events Checklist (Table F11.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for reconstructing past events. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Recovering electronic data is only the beginning.
2. True or False? Even if the data is in a format that appears to be one you already use, conversion may not be necessary.
3. True or False? If you are going to attempt converting the data yourself, you may be fortunate enough to have received electronic data that you can convert directly into programs such as Access or Excel using the wizards built into those programs.
4. True or False? Once the data has been unsuccessfully collected, it must be analyzed to extract the evidence you wish to present and to rebuild what actually happened.
5. True or False? Refining the firewall rules, keeping the IDS current, and reviewing the log files will be important to stay one step ahead of the bad guys.

Multiple Choice

1. The increase in computer-related crime has led to development of special tools to recover and analyze what?

   A. NRA
   B. Computer data
   C. Search data
   D. Data specialists
   E. Data centers

2. Today, data can come on a variety of:
   - A. Radio telescopes
   - B. Media
   - C. Radios that listen to time signals such as WWV
   - D. Global positioning system (GPS) receivers
   - E. Atomic clocks
3. Having data on a useable medium is useless unless it also is in a:
   - A. Rival's next move
   - B. Plot
   - C. Disaster
   - D. Unuseable format
   - E. Useable format
4. Hardware requirements will vary greatly depending on:
   - A. Computer files
   - B. File fragments
   - C. Timekeeping
   - D. Data miming
   - E. Specific circumstances
5. Electronic files often contain "hidden" data (information that does not show up on any printouts of the file) that can potentially prove to be:
   - A. Useful
   - B. Not useful
   - C. A waste of time
   - D. Good
   - E. Bad

Exercise

Offensive jokes were being posted in various locations in the offices of a large corporation. Management had identified four possible suspects but each denied involvement. The company's IT department could not find where the documents had been created on any computer in the office. A CFS team (CFST) was called to consult on the matter [2]. Using forensic analysis, how did the CFST solve the problem?

HANDS-ON PROJECTS

It was every attorney's nightmare. A default judgment had been entered against his client because no answer had been filed with the court. The attorney knew he had signed the paperwork and his paralegal insisted that the paperwork had been mailed to the court. However, the paralegal did not receive a stamped copy returned from the clerk and never followed up. The opposing counsel would not consent to re-opening the case, and the client had secured a hearing to attempt to set aside the judgment and re-open the case. A CFST was called in to perform a forensic analysis of the paralegal's computer to determine when the document had been created and last revised, hoping to verify her testimony [2]. What do you think the CFST did to resolve the case?

Case Projects

An executive at a company was accused of stealing or misdirecting company funds for his personal use. The company requested that a CFST process the computer in the subject's office to determine if any evidence of the theft was there [2]. What do you think the CFST found?

Optional Team Case Project

Three months after an application developer was fired from a major railroad company for harassing a female clerk, someone gained unauthorized remote access to the company's computer network, using the name and password of another employee. The intruder copied and then deleted almost 2,000 files relating to senior executive compensation, corrupted the compensation database to give the clerk a $250,000 raise, and tampered with audit trail information to disguise the date and time of the intrusion. Simultaneously, an intruder hacked into the clerk's personal, university email account, copied content from that account, established unauthorized Yahoo! and Hotmail accounts using the clerk's name, and began forwarding embarrassing content from the clerk's personal email box to the clerk's supervisors at the company. To make matters worse, the intruder physically stole another employee's two-way pager and, from it, began sending increasingly threatening emails to the clerk. What did the CFST do to solve this case?

REFERENCES

[1] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

[2] Mandall, Robert, Computer, Forensic Evidence Solutions, Inc. (© 2002 Computer Forensic Evidence Solutions, Inc.), 1212 Hope Ranch Lane, Las Vegas, NV 89134, 2002.

This page intentionally left blank

12 Networks

As information systems become cheaper and cheaper, companies are rapidly automating not only their overhead processes such as purchasing, payables, hiring, and payroll, but also their value by adding processing such as marketing and sales. The result of this rush to automate and, with the explosion of the Internet, a rush to publish, is the highest level of dependency on information systems corporate America has ever seen. With this dependency comes a vulnerability: The ability of corporations to conduct their business is dependent on technology that was designed to be as *open* as possible and that only a minority of engineers and scientists understand.

When connected to the Internet, what managers need to do is create barriers that deter cyber-based or internal perpetrators from attacking their systems. The first way to do this is to analyze corporate resources for known vulnerabilities. That is, systems need to be checked to ensure that they are correctly configured and have the most up-to-date security patches in place. This is what security scanners do. Next, one needs to find out the perpetrator's methods of operation and be alert when those methods are sensed. This is what intrusion detectors do. Next, one needs a mechanism to filter out suspected malicious activity once it is identified. This is what firewalls do. However, even with all of these systems in place, there is a vulnerability to attacks that use new or unknown methods.

What current intrusion detection systems (IDSs) do is monitor the network and watch for specific patterns. Once a pattern is recognized, the IDS can alert the systems administrator, close the connection via the firewall, or record the activity for further analysis. However, if an attacker uses a method not previously known to the IDS, it will transpire unnoticed, the corporate Web site will be defaced, employee records will be retrieved, or client lists will be extracted. When the malicious act is discovered, the question immediately comes to mind: How did they do this? And sometimes: What did they do?

This chapter introduces a solution to this dilemma: network forensics. Network forensics is the principle of reconstructing the activities leading to an event and determining the answers to "What did they do?" and "How did they do it?" Instead of matching observed activities on a local area network (LAN) to a database of known patterns of malicious intent, it records all activity on a LAN and provides centralized tools to analyze the activity in real time for surveillance and historically for damage assessment and prosecution. Because the system is network-based, it is impregnable to circumvention. If a resource is accessible via a LAN for exploitation, it is observable by a network forensics agent.

NETWORK FORENSICS SCENARIO

A high-profile computer system has been compromised, and federal law enforcement officials have been called in to investigate the break-in. Fortunately, a network security system has been retaining all network packet information for the past six months. Because of the high volume of data involved, advanced visual analysis tools are applied to the tens of millions of network events. These tools, in combination with information produced from an on-sight investigation, are used to identify suspect communications. Through the use of visualization tools, the investigators identified the intruder and his unlawful activity spanning six months. In addition, patterns of network misuse invisible to system administrators, caused by other perpetrators, were discovered through pattern analysis. The additional abnormalities in network usage were identified by visually mining through the forensic data.

A TECHNICAL APPROACH

One approach here will be to use an interactive visualization interface to drive the underlying network forensic data acquisition tools and analysis routines. The objective of the interface will be to capture the abilities of a skilled network security analyst into an intuitive and guided examination of network security events. To achieve this, you should propose to investigate different visualization techniques to model the network security data. The goal is to encapsulate these visualization techniques into modular network forensic data visualizers. In addition, you should tie these data visualizers into a visual query interface that can drive the network security database backend.

For example, a prototyping vehicle used to conceptualize and test these ideas is AVS/Express (*http://www.avs.com/software/soft_t/avsxps.html*). AVS/Express is a comprehensive and versatile data visualization tool for both non-programmers and experienced developers. Rapid data analysis and rich visualization techniques combined with an intuitive, graphical application development environment make AVS/Express the best choice for any data visualization task. AVS/Express provides powerful visualization methods for challenging problems in a vast range of fields, including science, business, engineering, medicine, telecommunications, and environmental research. Also, an interactive data flow process allows multiple visualization steps to be combined as a single visualization macro. The main components of a network forensic data visualizer are as follows:

- Network forensic data and database
- Visual query interface
- Network forensic data visualizers

AVS/Express is Advanced Visual System's [1] visualization development tool. It is a modular, hierarchical, open, and extensible system with hundreds of predefined components for visualizing data.

Network Forensic Data and Database

The data that will be used for visual analysis consists of network forensic data describing Internet protocol (IP) sessions. This data can consist of, but is not limited to, a time, date, IP address pair, session type, and duration. Session type identifies the communication event type. For example, network communications such as email, ftp transfers, and http sessions are considered to be session types.

The collected network communication metadata should be stored in a high-capacity data warehouse. The data warehouse should consist of the following two stages: stage 1 collects all observed network transactions and records them into logs; stage 2 summarizes these transactions into objects and communicants producing a network event. You should also investigate the possibility of creating additional smaller *browsable* tables for supporting rapid high-level looks into the database. If successful, these will support a smooth interactive visual query interface while still allowing drilling down into the more extensive databases with additional, more extensive queries.

Currently there are various reports that can be generated on these databases via queries. One approach to integrate these reports into the visualization engine is to develop network forensic data models that can hold the different types of report data and provide a seamless input into the visualization engine through data readers. Thus, to integrate a new report type into the visualization engine, you must first create a predefined query as a data model or a variation on an existing data model that is created for the report, where the data is inserted into the data model and a reader is developed to load the data model into the visualization engine.

Visual Query Interface

The visual query interface allows the network security analyst to interactively probe the output of the network forensic data visualizers. A probe may involve one of several different actions. One is to expose greater detail at a particular data point. For example, if the node of a network security event is shown, then picking it would give the ancillary information associated with that node. Second, one may use node information as a way to give additional constraints to a drill down query. This would allow, for example, a way to pare down the number of nodes that need to be examined. An effective data visualization is highly segregated by space and color. Therefore, spatially oriented visual queries can serve to partition the data space and be automatically translated to query constraints. Range constraints can be applied based on the node data or color values. Finally, a menu-driven choice of a set of predefined queries can help serve as a navigational aid into the various parts of the database.

The goal here is to investigate the effectiveness of each of the preceding techniques in browsing and navigating the network forensics database. Effective techniques can then be incorporated as templates to allow the network security analyst to customize the interface to perform context-based searches pertinent to his or her investigation.

Network Forensic Data Visualizers

Network forensic data visualizers are key to an understanding of the network forensic data. They not only allow the raw network data to be displayed, but do so in a way that highlights relevant data through spatial, color, or projection techniques. You should also investigate a number of different visualizations of the network forensic data to see which methods work best in conveying useful information to the network forensic analyst. Due to the large size of the network forensic database, a hierarchical approach may be useful in categorizing the visualizations, with each level showing correspondingly greater detail. Such an approach could also support the visual query interface in a browse/detail mode. You should also investigate such a hierarchical partitioning of detail to see if it can be used as an effective means of displaying network forensic data at different detail levels.

The network forensic database also has several possibly different modes of investigation. The first looks at the data from a chronological or time-ordered point of view. In this case, the visualization performs a mapping from time-ordered to space-ordered view or presents a specific time range with other parameters such as duration, ip_address, and session type being mapped spatially. In addition, binning (see note below) to create counts of events within certain ranges of parameters is also possible.

NOTE

Binning is a method used to map data to spatial axes in uniformly sized bins. Real values are discretized into data ranges that define a bin. Unique categorical values define a bin. Binning resolution determines accuracy and rendering efficiency.

In the second mode of investigation, a network-event view of the database is appropriate. This can lead to a nodal map view of the network events. Connections could represent paths an intruder has used to enter the network domain.

DESTRUCTION OF EMAIL

Now that email has worked its way into the very fabric of your life, you need to recognize it as more than simply an informal, casual means of communication. The courts treat email as formal records—no different than print communication—so be prepared for the legal consequences, including the fact that your company's email is discoverable in litigation.

For example, just ask Bill Gates about the significance of this treatment. Reams and megabytes of Microsoft email messages dating from the 1990s (including Gates' own) were used skillfully by the government in its antitrust case against Microsoft. As with any other printed documents, these email messages were deemed records discoverable under the federal rules of civil procedure.

Accordingly, the courts will not hesitate to compel businesses to produce these records and, further, to sanction them for their failure to do so. For instance, in the Brand Name Prescription Drugs Antitrust Litigation, 1995 WL 360526 (N.D. Ill. 1995), the court required the corporate defendant, CIBA-Geigy Corporation, to produce over 30 million email messages stored on backup tapes and to foot the $50,000–$70,000 cost of searching the messages and formatting them into a readable form. According to the court, the reasonable translation of electronic data into a usable form is an ordinary and foreseeable burden of litigation that the defendant should bear, absent a showing of extraordinary hardship.

That the electronic data may be duplicative of print documentation already produced in litigation is irrelevant. Thus, for example, when the insurance company in American Bankers Ins. Co. of Florida v. Caruth, et al., 786 S.W.2d 427 (Tex. Ct. App. 1990) failed to produce computer files despite already having produced approximately 30,000 boxes of material containing the same information, the court sanctioned the company by conclusively deeming each allegation against the company to be true, thereby precluding the company from contesting the allegations and leading to a default judgment against it.

Hitting the Delete button on your keyboard is not a panacea either. Do you remember Oliver North, whose deleted email messages from the White House were retrieved from a main frame backup tape during the Iran-Contra investigation? If information that has been deleted has not yet been overwritten by the computer system or is stored on back-up tapes or archive tapes, the information may still be accessible.

Any attempts to destroy the email will likewise be met with harsh consequences. For example, in Computer Associates International, Inc. v. American Fundware, Inc., 133 F.R.D. 166 (D. Colo. 1990), a developer of a computer program, over the course of years, destroyed prior versions of a source code, retaining only the current version. Although the court acknowledged that such destruction of older versions may be the standard industry practice, the court found that once the developer knew, or should have known, that the source code would probably be critical evidence in pending or imminent litigation, a duty arose to preserve it. The court held that the developer had received a copy of the lawsuit filed by the holder of the copyright to the computer program but continued to destroy older versions of the source code. Therefore, the developer had breached his or her duty to preserve the code. Accordingly, the court entered default judgment against the developer as an appropriate sanction.

Employers beware, for even prelitigation correspondence has been found sufficient to impose a duty to preserve relevant documents, electronic or otherwise (see the example of William T. Thompson Co. v. Gen'l Nutrition Corp., 593 F. Supp. 1443, 1446 [C.D. Cal. 1984]). Recently, one court imposed a $1 million sanction, as well as reimbursement of attorney fees, even though no willful destruction of electronic records was found (see the example of re Prudential Insurance Co. Sales Practices Litigation, 169 F.R.D. 598 [D.N.J. 1997]).

To avoid these litigation nightmares, you should implement a consistent retention policy that includes one or more of the following: routinely archive all email as it is received on your server for a certain period of time (for example, 30–60 days); clear the archives after an additional specified time; physically segregate the backup copies of the email system from backups of the rest of the computer system; automatically erase email from the computer system, including backups, after a short period (15–30 days); apply uniform retention and deletion standards and features outside the server to workstations and laptops; and formulate and distribute a statement that the automatic deletion of electronic records will be suspended and steps taken to preserve records in the event of investigation or litigation. With such a policy in place, you may not stay out of the courtroom, but at least you will be prepared if you ever find your company the target of a lawsuit or subpoena.

Now, let's look at the development of cross-disciplinary guidelines and standards for the recovery, preservation, and examination of digital evidence, including audio, imaging, and electronic devices with regard to the damaging of computer evidence. This part of the chapter proposes the establishment of standards for the exchange of digital evidence between sovereign nations and is intended to elicit constructive discussion regarding the damaging of digital evidence.

DAMAGING COMPUTER EVIDENCE

To ensure that digital evidence is collected, preserved, examined, and transferred in a manner that safeguards its accuracy and reliability, law enforcement and forensic organizations must establish and maintain an effective quality system. Standard operating procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and use broadly accepted procedures, equipment, and materials.

The use of SOPs is fundamental to both law enforcement and forensic science. Guidelines that are consistent with scientific and legal principles are essential to the acceptance of results and conclusions by courts and other agencies. The development and implementation of these SOPs must be under an agency's management authority.

Rapid technological changes are the hallmark of digital evidence, with the types, formats, and methods for seizing and examining digital evidence changing quickly. To ensure that personnel, training, equipment, and procedures continue to be appropriate and effective, management must review and update SOP documents annually.

Because a variety of scientific procedures may validly be applied to a given problem, standards and criteria for assessing procedures need to remain flexible. The validity of a procedure may be established by demonstrating the accuracy and reliability of specific techniques. In the digital evidence area, peer review of SOPs by other agencies may be useful.

Procedures should set forth their purpose and appropriate application. Required elements such as hardware and software must be listed, and the proper steps for successful use should be listed or discussed. Any limitations in the use of the procedure or the use or interpretation of the results should be established. Personnel who use these procedures must be familiar with them and have them available for reference.

Although many acceptable procedures may be used to perform a task, considerable variation among cases requires that personnel have the flexibility to exercise judgment in selecting a method appropriate to the problem. Hardware used in the seizure and examination of digital evidence should be in good operating condition and be tested to ensure that it operates correctly. Software must be tested to ensure that it produces reliable results for use in seizure and examination.

In general, documentation to support conclusions must be such that, in the absence of the originator, another competent person could evaluate what was done, interpret the data, and arrive at the same conclusions as the originator. The requirement for evidence reliability necessitates a chain of custody for all items of evidence. Chain-of-custody documentation must be maintained for all digital evidence.

Case notes and records of observations must be of a permanent nature. Handwritten notes and observations must be in ink, not pencil, although pencil (including color) may be appropriate for diagrams or making tracings. Any corrections to notes must be made by an initialed, single strikeout; nothing in the handwritten information should be obliterated or erased. Notes and records should be authenticated by handwritten signatures, initials, digital signatures, or other marking systems.

Evidence has value only if it can be shown to be accurate, reliable, and controlled. A quality forensic program consists of properly trained personnel and appropriate equipment, software, and procedures to collectively ensure these attributes.

International Principles Against Damaging of Computer Evidence

The International Organization on Computer Evidence (IOCE) was established in 1995 to provide international law enforcement agencies a forum for the exchange of information concerning computer crime investigation and other computer-related forensic issues. Composed of accredited government agencies involved in computer forensic investigations, the IOCE identifies and discusses issues of interest to its constituents, facilitates the international dissemination of information, and develops recommendations for consideration by its member agencies. In addition to formulating computer evidence standards, the IOCE develops communications services between member agencies and holds conferences geared toward the establishment of working relationships.

In response to the G-8 Communique and Action plans of 1997, the IOCE was tasked with the development of international standards for the exchange and recovery of undamaged electronic evidence. Working groups in Canada, Europe, the United Kingdom, and the United States have been formed to address this standardization of computer evidence.

During the International Hi-Tech Crime and Forensics Conference (IHCFC) of October 1999, the IOCE held meetings and a workshop that reviewed the United Kingdom Good Practice Guide and the Scientific Working Group on Digital Evidence (SWGDE) Draft Standards. The working group proposed the following principles, which were approved unanimously by the IOCE delegates present. The international principles developed by the IOCE for the standardized recovery of computer-based evidence are governed by the following attributes:

- Consistency with all legal systems
- Allowance for the use of a common language
- Durability
- Ability to cross international boundaries
- Ability to instill confidence in the integrity of evidence
- Applicability to all forensic evidence
- Applicability at every level, including that of individual, agency, and country [2]

Furthermore, the following international principles were presented, approved, and approved again at the IHCFCs in October 1999 and 2001, respectively.

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in his possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles [2].

So, do you have a well-documented intrusion-detection response plan? In other words, if you are attacked, do you have the documentation tools that are needed to record the attack, so that you can make the proper response? Let's take a look.

TOOLS NEEDED FOR INTRUSION RESPONSE TO THE DESTRUCTION OF DATA

It is very important to document and inventory the tools needed for intrusion response to the destruction of data—including intrusion detection software, backups, and file-system-recovery tools. There is also a need to have written requirements for training IT staff on how to deal with intrusions. This can be System Administration, Networking, and Security Institute (SANS) courses, Computer Emergency Response Team's (CERT) Software Engineering Institute, training offered for your intrusion detection tools, or even custom training developed in-house. Training should also include some form of regular fire drill.

Incident Reporting and Contact Forms

Documenting the intrusion (incident) on destruction of data is very important, not only as an aid for solving the intrusion problem, but also for an audit trail that may even be used in criminal proceedings. It is critical to capture as much information as possible and create forms enabling users who are not intrusion detection specialists to provide as much information as possible. Some of the important elements of incident reporting forms are

- Contact information for person(s) discovering problem and responsible parties.
- Target systems and networks. Know all about the systems under attack, including operating system versions, IP addresses, and so on.

- Purpose of systems under attack. Know what the systems are used for (payroll, R&D, and so on), as well as some kind of a ranking of the importance of the system.
- Evidence of intrusion. Discover anything that is known about the intrusion, method of attacks used, source IP address of attacker, and network contact information for this address.
- List of parties to notify. This can include the technical contacts, internal legal contacts, and possibly the legal authorities.

Finally, when it comes to hardening your network against hackers, the best defense is to keep abreast of developing threats and to test your system with due diligence. In other words, you need to seal off the leaks.

SYSTEM TESTING

It seems you can't open a newspaper or listen to the news these days without learning that yet another company's network has been broken in to. The truth is that resilient new viral strains are popping up every day. Even worse, thanks to the advent of always-on DSL, ISDN, and cable modem connections, security breaches that were once limited to large corporations or government facilities are now finding their way into your homes as well.

Is your network vulnerable? If you do business on the Web or maintain a connection to an outside network, chances are that the answer is yes. Fortunately, it's not hard to decrease the odds of attack or intrusion. Statistics show that more than 82% of successful hacks occur because Web technicians fail to install patches for known and publicized bugs. In other words, a little effort can go a long way toward securing your network.

Domain Name Service

If you've ever used a URL to represent an IP address, you've used domain name service (DNS)—a distributed database that provides translation capabilities between domain names and IP addresses. DNSs also provide a standard Internet mechanism for storing and accessing other types of data, such as MX (mail exchange) records.

The Internet couldn't operate without DNSs, but the service is also rife with holes, especially on Unix implementations that use the Berkeley Internet Name Domain (BIND) variant of DNS. Designed to be a robust, stable system on which to build a sound organizational naming architecture, BIND (especially in its earliest versions) is notorious for its vulnerabilities. In fact, CERT, a federally funded security research and development center operated by Carnegie Mellon University, has declared that all BIND releases prior to Version 8.2.3 are likely to contain hazardous security holes.

To make matters worse, network intrusion programs that automatically scan networks and query corporate DNS servers looking for holes are becoming increasingly available to hackers, who use these programs to test a system's locks the way a traditional burglar might jiggle a doorknob. These programs, which can be found on most hacker or "cracker" Web sites, require little technical skill.

Once compromised, the DNS server can be used to launch disturbances such as distributed DoS (denial of service) attacks to disrupt your business. Thankfully, all it takes is a bit of housekeeping to reduce your chances of becoming a victim. First, if yours is one of the many companies that runs outdated DNS software, an upgrade is definitely in order. Install the latest version of your DNS software immediately.

Your next step should be to limit your access to port 53 (the DNS port) on your firewalls. Although User Datagram Protocol (UDP) packets are required for requests to and from the Internet DNS, your network's transmission control protocol (TCP) transport layer should be locked down except in cases when it's absolutely required, such as on primary and secondary servers at opposite sides of the firewall.

Services and File Sharing

Although services and file sharing capabilities are available on both Windows and Unix, Windows computers receive the brunt of file sharing attacks from trojan horses and share compromises. Many network administrators use share services to make data access more convenient, but hackers will often compromise healthy machines by installing backdoor programs that register themselves as share services when users start their systems. These shares can then be run from any client machine with "log on as service" rights.

To prevent unauthorized access through your network services, identify and remove all services that are not absolutely necessary. Doing so will also improve network performance. The same rule applies to new services, especially those that begin automatically at system startup. Nothing extraneous should ever be put into use.

File shares present another potential vulnerability to your network because, when improperly configured, they can expose critical system files or even give full file system access to any party that is able to connect to your network. Because Windows' file-sharing service uses NetBIOS, the same mechanism that permits file sharing can also be used to retrieve sensitive system information, such as user names, configuration information, and certain registry keys, via a "null session" connection to the NetBIOS session service. Information can then be leveraged to allow password guessing or a brute-force password attack against the Windows NT target.

Again, your best defense is diligence. Don't share files indiscriminately, and when you have no other choice, be sure to share only the files that absolutely must be shared. Granted, it's much easier to share an entire directory or forbid an entire drive, but the extra effort necessary to provide more granular access privileges will be well worth it.

Finally, bear in mind that, no matter how carefully you secure your network, dedicated hackers will always find a way to get in. Even security experts readily admit that firewalls and anti-virus procedures can offer only casual, "business as usual" protection. Malicious hackers have gone so far as to bribe insiders to steal corporate data. There's no way to secure your network against those kinds of attacks. On the other hand, casual hacking attempts present the greatest danger, if only because they're far more common. Any protection is better than none.

SUMMARY

This chapter introduced several solutions to the dilemma of network forensics. As previously explained, network forensics is the principle of reconstructing the activities leading to an event and determining the answer to What did they do? and How did they do it? Protecting your network against hackers need not be a full-time job. By including a few best practices as part of your organization's daily routine, you can prevent leaks from developing—or at the very least, plug them before the dams break altogether.

Conclusions

- One approach to network intrusion detection and network forensics depends on the development of new data visualization techniques to address the volumes of data collected in a forensics application.
- An algorithm used to reasonably collect and retain information about each and every packet that transits a network is needed. This comprehensive collection posture results in very large datasets that necessitate the use of data visualization techniques to reasonably analyze events.
- Visualization software should be produced to present the IP sessions in a manner that enables visual data mining. This will consist of gaining an understanding of IP session attributes, mapping these attributes to visual resources (x-axis, y-axis, z-axis, color, shape, thickness, etc.), establishing the connections to the datasets, and constructing dynamic, data-driven visualization displays.
- The resulting visualizations should allow an analyst with a cursory understanding of data networks to identify normal patterns of network traffic and therefore identify deviations from the norm.

- The visualizations should allow an analyst to drill through the volumes of data from the global view down to individual events or transactions.
- Different visualizations will be explored with ease of use and data density as the evaluation criteria.
- Acquisition of digital evidence begins with information or physical items that are collected or stored for examination purposes.
- The term *evidence* implies that the collector of evidence is recognized by the courts.
- The process of collecting is also assumed to be a legal process that adheres to the rules of evidence in that locality.
- A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee.
- Data objects are objects or information of potential probative value that are associated with physical items.
- Data objects may occur in different formats without altering the original information.
- Digital evidence is information of probative value stored or transmitted in digital form.
- Physical items are items on which data objects or information may be stored or through which data objects are transferred.
- Original digital evidence is physical items and the data objects associated with such items at the time of acquisition or seizure.
- Duplicate digital evidence is an accurate digital reproduction of all data objects contained on an original physical item.
- Copy is an accurate reproduction of information contained on an original physical item, independent of the original physical item.
- With forensic competency, there is a need to generate an agreement on international accreditation and the validation of tools, techniques, and training.
- Issues need to be resolved that relate to practices and procedures for the examination of digital evidence.
- The sharing of information that relates to high-tech crime and forensic computing is needed, such as events, tools, and techniques.
- Simple network management protocol (SNMP) is an extremely useful feature for recording system error messages from servers and routers, but it can also reveal quite a bit of information about your network.
- With the volume of network traffic increasing every day, network security remains a top priority. Most instances of unauthorized access result from simple negligence, so if all your company does is pay attention and adhere to a few basic routines, you'll already be ahead of the game.

An Agenda for Action

When completing the Networks Checklist (Table F12.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for networks. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? The data that will be used for visual analysis consists of network forensic data describing SNMP sessions.
2. True or False? The collected network communication metadata should be stored in a high-capacity data warehouse.
3. True or False? The visual query interface does not allow the network security analyst to interactively probe the output of the network forensic data visualizers.
4. True or False? Network forensic data visualizers are key to an understanding of the network forensic data.
5. True or False? To ensure that digital evidence is collected, preserved, examined, and transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations should not establish and maintain an effective quality system.

Multiple Choice

1. The main components of a network forensic data visualizer are as follows, except for two:
   A. Network forensic data and database
   B. Visual query interface
   C. Network forensic data visualizers
   D. Network forensic interaction
   E. Visual query data

2. The international principles developed by the IOCE for the standardized recovery of computer-based evidence are governed by the following attributes, except:
   - A. Consistency with all legal systems
   - B. Allowance for the use of a common language
   - C. Fragility
   - D. Ability to cross international boundaries
   - E. Ability to instill confidence in the integrity of evidence

3. The international principles discussed in question 2 were presented, approved, and approved again at the International Hi-Tech Crime and Forensics Conferences in October 1999 and 2001, respectively. They are as follows, except:
   - A. Upon seizing digital evidence, actions taken should change that evidence.
   - B. When it is necessary for a person to access original digital evidence, that person must be forensically competent.
   - C. All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
   - D. An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in his possession.
   - E. Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

4. The following are some of the important elements of incident reporting forms, except:
   - A. Private information for person(s) discovering problem and responsible parties.
   - B. Target systems and networks. Know all about the systems under attack, including operating system versions, IP addresses, and so on.
   - C. Purpose of systems under attack. Know what systems are used for (payroll, R&D, and so on), as well as some kind of a ranking of the importance of the system.
   - D. Evidence of intrusion. Discover anything that is known about the intrusion, method of attacks used, source IP address of attacker, and network contact information for this address.
   - E. List of parties to notify. This can include the technical contacts, internal legal contacts, and possibly the legal authorities.

5. What current intrusion detection systems (IDSs) do is monitor the network and watch for:
   - A. Usefulness
   - B. Specific patterns
   - C. Waste of time

D. Good patterns
E. Bad patterns

Exercise

A CFS team's (CFST) forensic work regarding the authenticity of a critical piece of electronic evidence led to the resolution of a multibillion dollar litigation. In the litigation, the version of the email in the sender's possession was silent on the issue of certain contract terms. The recipient's version of the email explicitly confirmed those same contract terms. It was alleged that one of the parties had tampered with its electronic record, which had been sent from a Lotus Notes environment into a Microsoft Outlook environment. A CFST was retained to determine "who dunnit." So, how were they able to determine "who dunnit?"

HANDS-ON PROJECTS

When the CEO of a major company opened his email one morning, he was shocked to see that overseas hackers were sending him confidential files from his own desktop hard drive. The hacker demanded hundreds of thousands of dollars as a "consulting fee," and threatened to disclose the information and the weaknesses in the company's security if the money was not paid. A CFST, working with the client's network personnel, preserved the evidence of the attack and assisted in determining how the attack occurred. How do you think they went about doing that?

Case Project

A major foreign investment company became very concerned when its IT staff determined one Monday morning that a recently terminated trader had gained unauthorized entry into the company's computer system over the weekend. The company's firewall logs indicated that the employee had downloaded terabytes of data, and audit logs indicated that he had corrupted several production databases. It also appeared that modem scripts on the trading floor had been sabotaged. A CFST was called in to solve the problem. Explain how you think they solved the problem.

Optional Team Case Project

In March 2004, one of the largest independent Internet securities trading firms contacted a CFST with a critical problem. For three days, someone had been targeting the firm with denial-of-service attacks, sending packets of data from a remote location that caused the firm's servers to crash for hours at a time. The company suspected an employee, a database programmer who had stormed out of the business three days before, unhappy with his severance negotiations. Given the nature of the firm's business, a prolonged denial of service would have crippled the firm, while also straining the ability of the firm's customers to do business. Please explain how the CFST went about solving this problem.

REFERENCES

[1] Advanced Visual System, World Headquarters, 300 Fifth Avenue, Waltham, MA 02451, 2002.

[2] U.S. Department of Justice, Federal Bureau of Investigation, J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW, Washington, D.C. 20535-0001, 2002.

This page intentionally left blank

Part IV

Countermeasures: Information Warfare

The fourth part of this book discusses how to fight against macro threats, defensive strategies for governments and industry groups, the information warfare arsenal and tactics of the military, the information warfare arsenal and tactics of terrorists and rogues, the information warfare arsenal and tactics of private companies, the information warfare arsenal of the future, surveillance tools for information warfare of the future, and civilian causalities (the victims and refugees of information warfare).

This page intentionally left blank

13 Fighting Against Macro Threats: Defensive Strategies for Governments and Industry Groups

Information warfare (IW), or sneak electronic assaults, could easily crash power grids, financial networks, transportation systems, and telecommunications, among other vital services. The National Security Agency (NSA) traces the macro threat from hostile or potentially hostile governments as well as drug lords, criminal cartels, and increasingly computer-savvy guerrilla groups. Some of these rogue organizations are doing reconnaissance today on U.S. networks, mapping them, and looking for vulnerabilities.

Cyberblitzes like those that briefly knocked out major Web sites a few yeas ago (including Yahoo! Inc.'s Internet gateway, eBay Inc.'s auction service, and Amazon.com Inc.'s retail site) could easily be copied on a larger scale. Criminals, crackers, foreign governments could all use this technique. And if it should happen, a future President had better move faster than Bush did during those infamous 7 minutes of pondering what to do when told of the 9-11 attacks.

Such warnings are not new for the agents at NSA, who have frequently conjured up a "digital Pearl Harbor," a reference to the Japanese surprise attack that threw the United States into the Second World War. The NSA and other U.S. officials seem to be stepping up a public awareness campaign, spurred by the spread of information technology, growing knowledge of malicious computer code, and ever greater U.S. reliance on networked systems.

IS THE U.S. GOVERNMENT PREPARED FOR INFORMATION WARFARE?

The answer is a resounding "no." A reasonable question that should be asked is "Why are we vulnerable?" In a recent report, the Defense Science Board Task Force on Information Warfare, lays the blame at the U.S. government's own doorstep.

The reality is that the vulnerability of the Department of Defense (and of the nation) to offensive IW attack is largely a self-created problem. Program by program, economic sector by economic sector, the U.S. government has based critical functions on inadequately protected telecomputing services. In aggregate, the U.S. government created a target-rich environment, and U.S. industry has sold globally much of the generic technology that can be used to strike these targets. From the standpoint of psychological operations, it's not so much exploited technology as it is that the U.S. government has created a global information system it does not control and does not understand, and this in turn creates additional targets for exploitation. Most recently, this problem is being exacerbated by the growing emergence of "always-on" connections being made to individual homes and small businesses.

Recently, for example, a private security company alerted the FBI that it found a malicious program on some 3,000 computers that could be remotely activated to launch an attack on a site of choice—a trojan horse. Many of these computers are privately owned and are on cable-modem or digital line subscriber (DSL) always-on connections. In addition to the technological risk posed by many of these computers having very limited or no security, the users of these computers often are attractive targets for social engineering efforts for a simple reason. The very thought that they would be targeted for an attack is unbelievable to them.

From an IW perspective, there are three primary target for the attacker using psychological operations (psyops). The attacker can focus on the enemy, those who are friendly to his or her cause, or those who are neutral, with each target chosen for a specific purpose. If the attacker is simply a hacker, cracker, or script-kiddie, it might be for nothing more than to grab a credit card number or prove to friends that he or she could do it. Unfortunately, the dangers the U.S. government faces are not limited to those groups. The government also faces the threat of multinational efforts to subvert their defenses and find an economic, diplomatic, or military advantage. These efforts might be aimed not only at the U.S. defense structure, but also at the U.S. utility infrastructure, transportation, communications, finance, and much more. The U.S. government also cannot discount the potential entrance of organized crime into the equation, not to mention political activists and disgruntled employees.

As more individuals (the neutrals) turn to the Internet to help them with tasks that have usually been served by personal service or other traditional means, tasks such as banking, tax filing, shopping, and personal communications, the Internet as a loci for commerce and communication becomes increasingly critical both to the individual and to the businesses and industries that serve the individual. Although the commercial sector is beginning to realize the importance of security, the information on virtually unprotected personal machines may very well hold the key to a crippling attack on any sector simply because those sectors exist to allow the personal machines to connect to do business.

From a psyops point of view, how is it done? In any attack, finding and exploiting a trust relationship can be a key to success for the attacker. One of the most often cited examples of a physical trust relationship that was exploited successfully is the Mitnick attack. Kevin Mitnick discovered a relationship between host A and host B. He was able to determine the probable response that host A would give to host B after receiving the initiating packet in a three-way handshake. He blocked host B with a denial-of-service attack and sent a packet to A crafted to look as if it came from B. He then sent the expected response along with a small payload that contaminated host A's .rhost file and caused host A at that point to completely trust Mitnick's computer. He dropped the attack on host B and simply accessed A as a trusted root user.

How might an attacker employ psyops against a trust relationship? One of the more common examples used to explain trust exploitation is that of the overworked call center. Imagine a worker at a large corporate call center. The caller has done some research and discovered that a new personal report has been commissioned by the CEO. He calls and identifies himself as Bert Jackson, who has just been hired by the boss. He tells him he's been working all day researching a project that the CEO wants a report on in the morning and he needs access to the system to put the report together. Unfortunately, he's forgotten his password and it's already 11 P.M. Can he get a new password or should he call the CEO and have him call? In a shop with strong security, that would be an easy call, but it's easy to see that, in many cases, the call center worker would simply trust that the caller is who he says he is and give out a new password. The net result? The attacker gets in and can probably hide his tracks before the real Bert Jackson complains.

If the company is also a prime contractor for the government, a public utility, or even a company whose success or failure can severely impact the stock market, then the attacker has gained a tremendous advantage by simply manipulating information he or she has gained by infiltrating the system. Assume for this scenario that a group wanted to create a deleterious impact on the stock market. That group, perhaps over a period of months, maps IP ranges that are known to belong to public Internet service providers (ISPs) providing high-speed, always-on access to individuals and small businesses and they map for the Netbios ports. As they map, a second team begins the infiltration process, finding machines that are unprotected and that contain information such as passwords to personal investment accounts, banking, and the like. Even though these passwords may be encrypted, with modern cracking tools being what they are, at the end of the mapping period, they very well could have discovered thousands of accounts, including Bert Jackson's, that could be exploited. Choosing the time to strike, they simultaneously use these accounts to issue massive sell orders to the various brokers and close thousands of bank accounts with the money transferred to offshore accounts that they may or may not care about accessing. The distributed nature of this attack would make detection and prevention difficult, if not impossible, and would certainly create an atmosphere of fear and distrust that would severely affect the general economy.

Again, the question is why? Let us look at the three basic types of attack: strategic, consolidation, and battlefield. If the preceding scenario were executed by organized crime, it would probably fall into the battlefield type because they probably would be looking to cause a drop in stock market prices where they could step in and buy cheaply, thus allowing them to see an impressive gain as confidence rebounded. If a foreign government perpetrated the attack, it might very well fall into one of the other two categories. The attackers might be trying to distract the attention of the current administration away from what they might be attempting elsewhere (strategic) or attempting to bring together the economic resources needed to launch a more serious battlefield attack against us later (consolidation).

What is it that causes you, as a whole, to make it easy for those who would want to abuse that trust? In a culture where the phrase “trust is earned” is a familiar maxim, it would seem that you would be more eager to challenge than you really are. However, trust also seems to be a social construct between two or more individuals. In both social and business milieus, a need to trust develops out of the need to foster cooperation to achieve goals and objectives.

If that is the case, then how does the U.S. government overcome this tendency and protect their critical resources? Part of the difficulty they face here is that their focus tends to be on strengthening the security of their physical defenses, whether that be through encryption, perimeter-based defenses, host-based defenses, or, preferably, a combination of the three. Unfortunately, the U.S. government still has too few people in system administrative positions who are security-aware enough to alter default installations on whatever machine they are setting up (whether it be Microsoft-based or Unix-based) to give an acceptable initial level of protection to their users. These are technological trust defenses and likely will always be open to attack. Although hardening those physical defenses is undeniably important, the U.S. government often overlooks the most dangerous vulnerability (their users), and that is where they spend the least amount of time in education. Why do computer viruses such as the “I Love You” virus of few years ago work? Because users, whether corporate, government, or private, haven’t been taught how to protect themselves and change the paradigm of automatically trusting the email that announces it comes from Aunt Barbara.

The U.S. government must begin focusing on the end user and on those who provide connections to the end users. When virtually all private connections to the Internet were made over modems connecting to a dynamic host configuration protocol (DHCP) server where each session was served with a different IP address, it was much less likely that a private machine would be compromised and efforts to compromise machines tended to be focused on commercial, government, and educational systems. Today, however, that situation is rapidly changing, and ISPs must accept the responsibility of advising their customers or requiring them to install personal firewalls [1] and giving them the advice needed to properly configure and maintain those firewalls. They also must understand the need to properly filter their outgoing traffic to block and detect activity coming from within their networks that can be harmful to the general Internet community.

Educating the end user is going to be the most daunting task. The recent proliferation of email-related viruses has certainly awakened many to the dangers, but there must be a broader effort to educate and assist users in protecting themselves and the U.S. government from the bad guys. To do this, the security community needs to do a better job educating first the media and then the public through the media. Psyops can work both ways. The difference between the U.S. government and the bad guys is that the government has permission—they have the intent to do what is right. So it is with perception management. The U.S. government can manage perception so people will realize the risks they face and take steps to protect themselves. In helping them to protect themselves, the U.S. government also helps protect the rest of the users on the Internet who could be attacked by their systems if they are compromised. Trust is wonderful when exercised in an environment where it is reasonable. In a global environment where criminals, unfriendly political forces, and people who just don't care about others have the same rights and access as anyone, trust can be dangerous.

Education, not legislation, is the key component. The U.S. government can pass all the laws it wishes, but it won't affect the traffic that is coming out of countries such as Korea, China, and Singapore. The government needs to communicate these messages with intelligence. If the U.S. government knows what needs to be done and doesn't communicate it effectively, then whatever else it does is irrelevant. If the government scattershots their communications without filtering them through an understanding of the message they need to convey, then all they are sending out is noise.

ARE OTHER GOVERNMENTS PREPARED FOR INFORMATION WARFARE?

Are other governments ready to use information-age tricks against their adversaries? Yes, to some extent. Case in point is as follows:

At first, the urgent phone call from the U.S. Transportation Department confounded Cheng Wang, a Long Island–based webmaster for Falun Gong, the spiritual movement that has unnerved Chinese authorities. Why did the department think his computers were attacking theirs? The answer turned out to be startling. The electronic blitz hadn't come, as it seemed, from various Falun Gong Internet sites.

Rather, someone had lifted their electronic identities. Computer sleuths followed a trail back to the XinAn Information Service Center in Beijing—where an operator identified it as part of the Ministry of Public Security, China's secret police.

Web hacking, it seems, isn't just for amateurs anymore. While the recent rash of cybervandalism against some of e-commerce's [2] biggest names has garnered headlines, that's only part of the story. From Beijing to Baku, governments and their surrogates are using the Internet to harrass political opponents and unfriendly neighbors, to go after trade secrets, and to prepare for outright warfare. Burma's military junta, for instance, is blamed for targeting the "Happy 99" email virus at opponents who use the Net to advance their cause. Dissidents describe the attacks as inept—proof, perhaps, that dictatorships are still behind the hacking curve.

Cyberwarfare

Burma is not alone in trying. In January 2000, hackers from Azerbaijan with names like "The Green Revenge" and "Hijack" tampered with dozens of Armenian-related Web sites, including host computers in the United States. Experts suspect involvement or support from the Azerbaijani government, which imposes tight controls over Internet use within its borders. Relations are tense between Azerbaijan and Armenia, who fought a war over the disputed territory of Nagorno-Karabakh, so it wasn't long before the Armenians retaliated in kind. It is the first case of a physical battle going online.

In Cheng Wang's case, his computers in Hauppauge, New York, were among the Falun Gong sites around the world hit by a barrage of hacking attempts and email "bombs" that coincided with a physical crackdown on the group's practitioners in China. Several of the hacking incidents were traced to the mysterious XinAn office.

It is often difficult to track down who is to blame, but for networked Americans, who own 60% of the world's computing capacity, such electronic conflict should be unsettling. True, the scariest scenarios dreamed up by experts, such as a hostile government disrupting financial markets, haven't come to pass—yet—but more than a dozen countries, among them Russia, China, Iraq, Iran, and Cuba, are developing significant IW capabilities. A senior CIA official cited a Russian general who compared the disruptive effects of a cyberattack on transportation or electrical grids to those of a nuclear weapon. China is considering whether to create a fourth branch of its armed services devoted to IW. The Pentagon isn't sitting still either. The U.S. military's offensive cyberwarfare programs are presently being consolidated at the U.S. Space Command in Colorado.

Nearly as worrisome as a cyberattack to experts is electronic espionage. From March 1998 until January 2001, intruders broke into computer systems belonging to the Pentagon, NASA, the Energy Department, and universities, making away with unclassified but still sensitive data. One of the worst computer security breaches in U.S. history that spawned an investigation was named Moonlight Maze. It pointed to a Russian intelligence-gathering operation.

Successful cyberwar is likely to be like that—no exploding munitions to tell someone they're under attack. Tapping into an adversary's command-and-control system could yield a gold mine of data about enemy plans. The longer a cyberspy conceals his or her presence, the longer the intelligence flows. Alternatively, false information about troop locations and battlefield conditions could be inserted into enemy computers, causing leaders to make decisions based on bogus information.

During the Kosovo bombing campaign in 1999, the Pentagon set up a high-level information-operations cell. All the tools were in place, but the United States mostly held back. By the time Pentagon lawyers approved cyberstrikes against Serbia, events had overtaken the need for them.

Disadvantages of Cyberwarfare

Cyberwar raises a host of unprecedented legal questions. The line between fair-game military sites and civilian infrastructure may not exist. There is collateral damage in cyberspace. If someone tampers with somebody else's control mechanisms, how assured are those individuals that it would stop right there? The United States, more dependent on computer networks than anyone, might lose the most in legitimizing cyberwar. Some countries, including Russia, have proposed what might be called "electronic arms control," but the obstacles are daunting: verifying a treaty would make counting Russian nuclear missiles look easy.

Among the sites hacked in the Caucasus Web war was one belonging to the Washington, D.C.–based Armenian National Institute, which studies the 1915–1918 Turkish genocide of Armenians. Logging onto *http://www.armenian-genocide.org* in late January 2000, one would have been redirected to a site offering information on Azerbaijan's president.

One Austin, Texas–based corporation already has its own rules. This corporation makes powerful search software for such uses as insurance-fraud investigations. The company will not license the technology to nine countries and three U.S. government agencies because of the potential for privacy abuse [3]. That hasn't stopped at least one of those countries from trying. In 1998, a company tried to buy rights to the technology. It turned out to be a front for the Chinese government.

WHAT INDUSTRY GROUPS HAVE DONE TO PREPARE FOR INFORMATION WARFARE

On December 18, 2000, the National Security Council held the first meeting of the recently formed Cyberincident Steering Group, aimed at fostering cooperation between private industry and government to secure systems from domestic and international cyberattack. This meeting was an important first step in building computer security programs for the nation. Among topics discussed were the creation of a rapid response system and communications between industry and government.

The U.S. intelligence community voiced its concerns with the release of "Global Trends 2015," a wide-ranging analysis by the CIA, its sister U.S. spy shops, and outside experts. According to the report, foes of a militarily dominant United States, rather than challenging it head-on, would seek to target an Achilles' heel in cyberspace or threaten the use of the deadliest chemical, nuclear, or biological weapons (see sidebar, "Doomsday Software").

DOOMSDAY SOFTWARE

After years of surveillance, Tokyo police thought they'd seen everything about Aum Shinrikyo, the high-tech doomsday sect behind the 1995 nerve-gas attack on that city's subway system, but even the cops were surprised after raiding cult facilities in February 2000 and finding evidence that Aum had developed software programs for at least 10 government agencies, including the Defense Ministry, as well as some 90 Japanese firms. With their identity hidden behind a web of front companies and subcontractors, Aum engineers sold as many as 200 systems ranging from databases for clients to an Internet messaging service.

Although no evidence has yet emerged that Aum installed so-called trapdoors to secretly gain access to its clients' data, authorities have reason to worry. In the mid-1990s, sect members burglarized and stole secrets from Japan's top defense contractor and its top semiconductor maker—part of an extraordinary campaign to develop biological agents, laser guns, and other high-tech weapons. Until now, Japan has shown an almost unbelievably low sense of its need for cybersecurity. That may soon change.

Such asymmetric approaches (whether undertaken by states or non-state actors) will become the dominant characteristic of most threats to the U.S. homeland. Over time, attacks are increasingly likely to be fired off through computer networks rather than conventional arms, as the skill of U.S. adversaries in employing them evolves.

FBI Fingers China

Many unnamed countries are developing technologies (previously discussed) to complicate what the U.S. military refers to as "power projection" and to undermine morale at home. The interagency, FBI-led National Infrastructure Protection Center, uses a slide depicting China's Great Wall in its standard presentation on cyberthreats, along with a quote from Sun Zi, author of a treatise on war in about 350 B.C. "Subjugating the enemy's army without fighting is the true pinnacle of excellence," the FBI's slide quotes the ancient Chinese strategist as saying. In a telltale update, the slide includes a 1999 quote from a Chinese newspaper referring to IW as a means of achieving strategic victory over a militarily superior enemy.

Industry Groups Prepare to Fight Cyberattacks

A group of technology heavyweights including Microsoft and Intel have recently unveiled a new resource in their efforts to strengthen cybersecurity. The group has established a new initiative through which high-tech companies can share information about the vulnerabilities in their software and hardware products. Participants in the undertaking, dubbed Information Technology Information Sharing and Analysis Center (IT-ISAC), exchange information about their security practices.

Board members of IT-ISAC have outlined the goals, mission, and operations of the new center. In attendance during the outline of the goals were representatives from Microsoft, AT&T, Oracle, IBM, Hewlett-Packard, Computer Associates, EDS, Entrust Technologies, KPMG Consulting, Cisco Systems [4], Nortel Networks, and other companies. Other organizations involved in the new center include the Information Technology Association of America, Veridian, Symantec, RSA Security, Securify, Titan Systems, and Verisign Global Registry Services. Members have created the center in hopes of improving responses to cyberattacks and hacking against corporate computer networks.

A number of giant companies, including Microsoft, have recently seen their corporate networks hacked. In such attacks, aimed at organizations large and small, some hackers may deface a Web site with graffiti or more pointed messages. Others toy with private information such as customer data and personal profiles. Many companies have increased security measures to safeguard valuable intellectual property, but a number of reports indicate that most continue to be vulnerable to such incidents.

According to a study by the American Society for Industrial Security (ASIS) and consulting firm Pricewaterhouse Coopers, Fortune 1000 companies sustained losses of more than $89 billion in 2003 from the theft of proprietary information—up from the late 1990s' estimates by the FBI that pegged the cost at roughly $57 billion a year. Tech companies reported the majority of those hacking incidents. The average tech company reported nearly 81 individual attacks, with the average theft resulting in about $59 million in lost business.

Following a string of attacks on federal systems, President Clinton in 2000 launched a $2 billion plan for combating cyberterrorism that included an educational initiative to recruit and train IT workers. The plan also included conducting federal agency vulnerability analyses and developing agency-critical infrastructure protection plans. With the aftermath of the 9-11 terrorist attacks, the Bush administration expanded this plan 50-fold.

STRATEGIC DIPLOMACY AND INFORMATION WARFARE

Strategic diplomacy, according to the Department of Defense, is the "art and science of developing and using political, economic, psychological, and military forces as necessary during peace and war, to afford the maximum support to policies, in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat." For most people, it is obvious that the political and economic aspects of the national security policies of the United States are developed by the national political authorities (the president and Congress) and, in dealing with foreign states or groups, executed by the Departments of State, Commerce, Agriculture, and so on.

Policies for developing and using military force are formulated by the national political authorities and conveyed to the armed forces through the secretary of defense. Few, however, pay much attention to just how and by whom psychological forces are to be developed to support national policies. More important, what are psychological forces? Who will use these forces? With what authority? To what ends?

New tools and technologies for communication have created the potential for a new form of psychological warfare to a degree imagined only in science fiction. This new form of warfare has become known as information warfare (IW). In other words, the United States armed forces need to develop a systematic, capstone concept of military knowledge and diplomatic strategy. Such a strategy would include clear doctrine and a policy for how the armed forces will acquire, process, distribute, and project knowledge.

The U.S. military is expanding the concept of IW to include psychological operations aimed at influencing the emotions, motives, objective reasoning, and, ultimately, the behavior of others. Such an expansion would mirror the evolution of traditional warfare toward IW. It would also mirror the progressive steps of generating wealth from agriculture and natural resources in much earlier times, to the 19th- and early-20th-century emphasis on industrial production, to the present emphasis on generating information products as a major new source of income. As "first wave" wars were fought for land and "second wave" wars were fought for control over productive capacity, the emerging "third wave" wars will be fought for control of knowledge. Because combat in any society follows the wealth-creation form of that society, wars of the future will increasingly be information wars.

Currently, there is neither formal military doctrine nor official definitions of IW. Despite the computer jargon involved, the idea of IW has not only captured the attention of military analysts but also posed important policy questions. Despite the lack of an authoritative definition, "netwar" and "cyberwar" are emerging as key concepts in discussing IW. Originally, these ideas seem to have come from the science fiction community.

Netwar is a societal-level ideational conflict waged in part through internetted modes of communication. That is, netwar is most likely to be a nation-against-nation strategic-level conflict. Netwar is about ideas and epistemology—what is known and how it is known. It would be waged largely through a society's communication systems.

The target of netwar is the human mind. One could argue that certain aspects of the cold war had the characteristics of a dress rehearsal for future netwar. Consider, for example, Radio Free Europe, the Cominform, Agence France Presse, or the U.S. Information Agency. Netwar, however, may involve more than traditional state-to-state conflict. The emerging of nongovernmental political actors such as Greenpeace and Amnesty International, as well as survivalist militias and Islamic revivalists, all with easy access to worldwide computer networks for the exchange of information or the coordination of political pressure on a national or global basis, suggests that governments may not be the only parties waging information wars.

At first glance, netwar may appear to be a new word for old-fashioned propaganda. It would be comforting to believe that the tried and true methods (and limitations) of propaganda still worked. The Gulf War showed that both Saddam Hussein and the Alliance were still of the old school. The war contained many elements of classic propaganda: accusations of bombed baby-milk factories and stolen baby incubators; inflated rhetoric and inflated stakes of the conflict; the future of the new world order and "the mother of battles" for the future of Islam; and the classic us or them polarization in which neutrality or unenthusiastic support was decried.

One element of traditional propaganda was absent, however. While Saddam Hussein became the new Hitler and President Bush, Sr. was the Great Satan, there was little demonization or dehumanization of the opponent soldiers. All of that changed, however, during the second invasion of Iraq in May of 2003 by George Bush, Jr.

Perhaps the multicultural nature of the American-led alliance precluded turning the Iraqi army into something subhuman. Indeed, there may have been a spark of netwar genius in treating the Islamic Iraqi soldiers as "brave men put into an impossible situation by a stupid leader." Under such conditions, there is no dishonor in surrendering. There may have been a glimpse of future netwar: it is rumored that Baghdad Radio signed on one morning with "The Star-Spangled Banner."

Traditional propaganda was usually targeted to influence a mass audience. Contemporary technologies have the potential to customize propaganda. Anyone who has received individually targeted advertising from a company specializing in niche marketing has had a momentary shudder upon realizing that some private companies seem to know everything about our tastes and buying habits. Contemporary databases and multiple channels for information transmission have created the opportunity for custom-tailored netwar attacks. Computer bulletin boards, cellular telephones, video cameras tied to fax machines—all provide entry points and dissemination networks for customized assault.

A major new factor in IW results directly from the worldwide infosphere of television and broadcast news. Many people have begun to realize that governmental decisions are becoming increasingly reactive to a "fictive" universe created by CNN and its various international competitors. This media-created universe is dubbed fictive rather than "fictional" because although what is shown may be true, it is not the whole, relevant, or contextual truth, and, of course, the close etymological relationship between fictive and fictional suggests how easy it is to manipulate the message.

Nevertheless, this fictive universe becomes the politically relevant universe in societies in which the government or its military is supposed to do something. Somalia gets in the news and the United States gets into Somalia despite the reality of equally disastrous starvation, disorder, and rapine right next door in Sudan. There were no reporters with skylink in Sudan because the government of Sudan issued no visas. The potential for governments, parties in a civil war such as Bosnia, rebels in Chiapis, or even non-state interests to manipulate the multimedia, multisource fictive universe to wage societal-level ideational conflicts should be obvious.

Fictive or fictional operational environments, then, whether mass-targeted or niche-targeted, can be generated, transmitted, distributed, or broadcast by governments or all sorts of other players through increasingly diversified networks. The niche-manipulation potential available to states or private interests with access to the universe of internetted communications, such as the networks over which business, commercial, and banking information are transmitted could easily provoke financial chaos. The target state would not know what had happened until too late.

Direct satellite broadcast to selected cable systems [5], analogous to central control of pay-per-view programs, again offers the potential for people in one province or region of a targeted state to discover that the highest level of their leadership has decided to purge their clansmen from the army. To put it in the jargon of the infowarriors, info-niche attack in an increasingly multisource fictive universe offers unlimited potential for societal-level netwar.

Fictive Broadcasts

When the new, but already well-understood, simulation technologies of the tekwar and MTV generation are added to the arsenal of netwar, a genuinely revolutionary transformation of propaganda and warfare becomes possible. Traditional propaganda might have attempted to discredit an adversary's news media showing, for example, that as the official casualty figures were demonstrably false, all news from the government was equally false. The credibility of the opponent was the target, and the strategic intention was to separate the government from the people.

Today, the mastery of the techniques of combining live actors with computer-generated video graphics can easily create a virtual news conference, summit meeting, or perhaps even a battle that exists in effects though not in fact. Stored video images can be recombined endlessly to produce any effect chosen [6]. Now, perhaps, pictures will be worth a thousand tanks.

Of course, truth will win out eventually, but by the time the people of the targeted nation discover that the nationwide broadcast of the conversation between the maximum leader and George W. Bush, in which all loyal citizens were told to cease fighting and return to their homes, was created in Hollywood or Langley, the war may be over. Netwar is beginning to enter the zone of illusion.

This is not science fiction; these are the capabilities of existing or rapidly emerging technologies. Here's how it might work: Through hitching a ride on an unsuspecting commercial satellite, a fictive simulation is broadcast. Simultaneously, various info-niches in the target state are accessed via the net. These info-niche targets, and the information they receive, are tailored to the strategic diplomacy needs of the moment: some receive reinforcement for the fictive simulation; others receive the real truth; still others receive slight variations. What is happening here?

This kind of manipulation elevates the strategic potential of infopropaganda to new heights. This is not traditional propaganda in which the target is discredited as a source of reliable information. Rather, the very possibility of truth is being replaced with virtual reality, that is, information that produces effects independent of its physical reality. What is being attacked in a strategic level netwar are not only the emotions, motives, or beliefs of the target population, but the very power of objective reasoning. This threatens the possibility of state control.

Let us return to the previous scenario to play out its effects. The fictive simulation of the maximum leader's call to stop fighting would, of course, be followed immediately by a real broadcast in which state exposes the netwar attack as propaganda invented by culture destroyers in Hollywood. George W. Bush is denounced as a hoax by the Internet blogs, but the damage has already been done: It is all but impossible for the television viewers of the targeted state to tell which broadcast is true and which is fiction, at least in a timely manner. In a society under assault across its entire infosphere, it will become increasingly difficult for people to verify internally the truth or accuracy of anything. Objective reasoning is threatened.

At the strategic level, the ability to observe is flooded by contradictory information and data; more important, the ability to orient is weakened by the assault on the possibility of objective reasoning; decisions are made increasingly in response to a fictive or virtual universe and, of course, governmental and military actions become increasingly chaotic, as there is no rational relationship of means to ends. It would seem, then, that strategic-level netwar or IW brings one within sight of that elusive acme of skill wherein the enemy is subdued without killing by attacking their ability to form a coherent strategy.

Reality, however, may be far more complex than the infowarriors yet imagine, and victory not so neat. The idea of societal-level ideational conflict may need to be considered with all the care given to the conduct of nuclear war, as the end state of netwar may be not bloodless surrender but total disruption of the targeted society. Victory may be too costly, as the cost may be truth itself.

Communication Truth

Any discussion of IW, netwar, cyberwar, or even perception manipulation as a component of command and control warfare by the armed forces of the United States at the strategic level must occur in the context of the moral nature of communication in a pluralistic, secular, and democratic society. That is, the question must be raised whether using the techniques of IW at the strategic level is compatible with American purposes and principles.

Likewise, the question must be raised whether the armed forces of the United States have either the moral or legal authority and, more important, the practical ability to develop and deploy the techniques of information warfare at the strategic level in a prudent and practical manner. There are good reasons to be skeptical.

The moral basis of communication in any society can be discussed in terms of its substantive, pragmatic, and intoxicant functions. The substantive purpose of communication is the building or developing of the individual human personality. It is simultaneously the process by which a substantive, real-world community of like-minded persons is created, developed, and sustained. It is the glue that binds a society together.

At the most trivial level, the moral purpose of substantive communication can be seen in contemporary American efforts to remove sexist or racist language from accepted use. At a more serious level, the debates in American society about prayer in the public schools illustrate a recognition of the substantive and formative nature of communication in society. This is true because many believe that private religious views must not corrupt the public school formation of character for life in pluralistic, modern America.

Finally, any real-world society rests on substantive communication and understanding among its members. Society is no mere external structure of relationships; it is a cosmion, a universe of meaning illuminated with meaning from within by the human beings who continuously create and bear it as the mode and condition of their self-realization.

The efforts of several nations such as China, Iran, and Saudi Arabia to insulate their societies from the effects of the global communications network, illustrate their awareness that their cultures and societies may depend on a distinctive shared, substantive universe of discourse. Even in the West, the French believe the continued existence of France as a distinctive society organized for action in history may require state intervention in the substantive content of communication within society. That France seeks to limit the percentage of foreign broadcast material and American films in Europe illustrates the seriousness with which they consider the substantive nature of communication.

Identifying the pragmatic function of communication in society is reasonably straightforward. Pragmatic communication is defined by its goal and consists of the universe of techniques designed to influence other persons to behave in ways the communicator wishes. Only behavior matters. Most political and commercial communication is merely pragmatic. It is usually indifferent to the substantive moral content of the communication and intends to mold perception, and, consequently, behavior, to the purposes of the communicator. This pragmatic use of communication as an attempt at perception manipulation is, of course, the central essence of IW. Its use by the government and the armed forces is, thus, the real issue.

Finally, the intoxicant function of communication in American society is equally straightforward. The addiction of a considerable part of the citizenry to talk shows, soap operas, romance novels, professional sports broadcasts, high-profile legal trials, and other well-known forms of distraction and diversion is well catered to by the entertainment industry.

Civil communication, or public discourse, in contemporary American society is dominated almost entirely by the intoxicant and pragmatic modes. More importantly, the absence of substantive communication in public life is defended by much of the secular and liberal political class in the name of freedom, pluralism, and multiculturalism.

Pluralistic America is supposed to be a society in which the formation of character and opinion is left, through the use of various means of communication, to private initiative. Government attempts at communication in an information war, especially if prosecuted by the armed forces, would raise serious questions in a pluralistic, multicultural society.

The official military view of diplomatic strategy is the art and science of developing and using political, economic, psychological, and military force as necessary during peace and war to afford the maximum support to policies, to increase the probabilities and favorable consequences of victory, and to lessen the chances of defeat. Diplomatic strategy is the means to an end, with military diplomatic strategy serving political or policy purposes. A slightly different view of strategy, however, may highlight a problem of IW. If strategy were seen as a plan of action designed to achieve some end, a purpose together with a system of measures for its accomplishment, the limitations of IW thinking are obvious.

Sound military strategy requires influencing the adversary decision maker in some way that is not only advantageous but also reasonably predictable. The goal is control, not chaos. A national security strategy of IW or netwar at the strategic level (that is, societal-level ideational conflict waged in part through internetted modes of communication) and an operational-level cyberwar or command-and-control warfare campaign to decapitate the enemy's command structure from its body of troops may or may not be advantageous but, more important, is unlikely to produce effects that are reasonably predictable.

Conflict is about a determinate something, not an indeterminate anything. If the goal is influencing the adversary's ability to observe by flooding them with corrupted or contradictory information and data, disrupting their ability to orient by eliminating the possibility of objective reasoning, and forcing their decisions to respond to a fictive or virtual universe, actions will, of course, be produced. However, they may well be actions that are chaotic, random, nonlinear, and inherently unpredictable, as there is no rational relationship of means to ends.

The military operational-level of cyberwar or command-and-control warfare appeals to the infowarrior as an attractive military strategy. Thus, the inherently unpredictable nature of combat, the notorious fog and friction of real battle, will be amplified for the enemy in a successful cyberwar.

A successful diplomatic cyberstrategy depends on the ability of the local military commander to deploy his or her power assets, especially combat forces, not merely to dominate the enemy's decision cycle (which, after all, has just been rendered chaotic), but to exploit opportunities as they evolve unpredictably from the disoriented, decapitated, or irrational enemy actions. Whether, then, command-and-control warfare can shape the battlefield or merely generate chaos remains to be seen.

Diplomatic cyberstrategy is the control of the evolution of the battlefield or theater power distribution to impose the allied commander's order on the enemy's chaos. The threat exists, however, that the destruction of enemy rationality may collapse battle into mere fighting with no outcome but surrender or death. Merely defeating hostile military forces may be insufficient.

Whether the Gulf War and the second invasion of Iraq were strategic victories or mere battles remains for historians to judge. Operational-level cyberwar may, then, be that very acme of skill that reduces the enemy will without killing. On the other hand, it may also be the abolition of strategy, as it attacks the rationality the enemy requires to decide to terminate the war.

Strategic Diplomatic Implications

The tools, techniques, and strategy of cyberwar will be developed and, during wartime, should be employed. In many ways, cyberwar is more demanding than netwar, but the resources, organization, and training needed for cyberwar will be provided once its war-winning, and casualty-reducing, potential is grasped by the national political leadership. Such a development would certainly be prudent. On the other hand, many of the tools and techniques of battlefield cyberwar can be applied to netwar or strategic-level IW. This application may not be prudent, however, as there are serious reasons to doubt the ability of the United States to prosecute an information war successfully.

One reason is that the United States is an open society; it may be too vulnerable to engage in netwar with an adversary prepared to fight back. Our communications infrastructure, the information highway, is wide open. American society may be terribly vulnerable to a strategic netwar attack; getting us to believe fictive claims appears to be what commercial and political advertising are all about, and they seem to be effective. Also, one may find physical control and security to be impossible. The domestic computer, communication, and information networks essential for the daily functioning of American society are vulnerable to penetration and manipulation (even destruction) by determined hackers. In the future, these may not be amateurs, but well-paid "network ninjas" inserting the latest French, Iranian, or Chinese virus into AOL or other parts of the Internet.

A strategic IW attack on America's communication systems, including our military communication systems, air traffic control system, financial net, fuel pipeline pumping software, and computer-based clock and timing systems, could result in societal paralysis. Currently, for example, over 101,000 Internet databases are being used by over 543 million people in over 163 nations. Over 44,500 software pirates are prowling the Internet, some in the employ of hostile commercial or intelligence services. The spy flap between France and the United States over alleged U.S. attempts to gather data on French Telecom may be indicative of the future.

Infosphere dominance (controlling the world of information exchange) may be as complex and elusive as escalation dominance appeared to be in nuclear strategy. It will certainly be expensive: the U.S. business community and the U.S. armed forces are required to devote ever more resources and attention to computer, communications, and database security. The resources and skills required for battlefield cyberwar are not insignificant, but the resources and skills required to wage an information war at the national strategic level would be massive.

The second reason to doubt U.S. ability to prosecute an information war is that the political and legal issues surrounding IW are murky. What of congressional oversight? Would one declare information war in response, say, to an Iranian-originated computer virus assault on the FBI's central terrorist database? What about preparing for it? How should the United States develop and implement a national capability for netwar?

Although, theoretically, a requirement to develop or implement a national IW strategy, analogous to the nuclear-era single-integrated operations plan, could be communicated from the president to the executive branch agencies, it is unclear whether there would be adequate congressional oversight. Which committees of the House or Senate would have control and oversight of policies attendant to IW? Which would have the power to inquire into the judgment of a local ambassador or military commander who wished to use the tools of cyberwar for a perception manipulation in peacetime that would shape the potential wartime environment?

The U.S. armed forces only execute the national military strategy—they do not control it. However, they are developing, quite appropriately, the tools and techniques to execute the national military strategy for operational-level cyberwar. They are simultaneously, albeit unintentionally, developing the tools and capabilities to execute a national strategic IW strategy. The former is their job under the

Constitution; the latter may not be. Congressional oversight of the development of a national strategic-level information war capability is even more essential than oversight of the intelligence community.

The third reason to doubt U.S. capabilities in prosecuting an effective information war is that such a societal-level ideational conflict waged in part through internetted modes of communication may simply be beyond the competence of the executive agencies that would have to determine the substantive content to be communicated. Pluralism is a great strength of American society but perhaps a drawback in waging information war.

Although diversity may make the formation and execution of domestic and even foreign policy more complex, the lack of a moral center or public philosophy in American society could render the political leadership incapable of building a consensus on strategic-level IW policies. Because there is no single view of what is morally acceptable, but simply a host of contending views, a national security strategy of IW could be developed by the national security decision makers who lacked a moral consensus.

Technological wizardry does not change the humanity of the target. Unless the goal of an information war is merely to unhinge people from their ability to reason objectively, and thereby create an interesting problem for post-conflict reconstruction, any strategic-level netwar or information war would require the ability to communicate a replacement for the discredited content of the target society.

If, for example, an information war were to be mounted against China to disrupt its drive for regional hegemony, the goal would be to withdraw the Mandate of Heaven from the rulers and influence the Chinese leaders and people to adopt the policies or behavior the United States finds appropriate. Put in terms of such a concrete policy goal, the philosophically problematic nature of information war becomes outrageously obvious. Does anyone really believe that the U.S. national executive agencies, including the armed forces and the CIA, know the substantive discourse of China sufficiently well to withdraw the Mandate of Heaven?

The final reason, then, can be stated in the form of a question: Does anyone really believe that anyone in the U.S. government has the philosophical sophistication to project an alternative discourse to replace the emotions, motives, reasoning, and behavior grounded in the Chinese reality that the United States proposes to influence? Would our fictive creation really have virtual effects? The United States might be able to use the armed forces or the CIA to destroy China's objective reasoning through a successful information war. Indeed, the United States might be able to loose anarchy in a society, but that is not usually the political goal of war.

Second Thoughts

The techniques the armed forces is developing for a more narrowly constrained operational-level cyberwar were demonstrated in the Gulf War and again in the second invasion of Iraq. Translated to the strategic level, however, netwar or information war is not a prudent national security or military strategy for the simple reason that neither the armed forces nor any other instruments of national power have the ability to exploit an adversary's society in a way that promises either advantageous or predictable results.

Societal-level ideational conflict must be considered with all the care given to the conduct of nuclear war, as the end state of a netwar may be total disruption of the targeted society. Conflict resolution, including ending wars this side of blasting people into unconditional surrender, assumes and requires some rationality—even if that rationality is the mere coordination of ends with means.

Moral reasoning and substantive communication may not be required; minimal reasoning and pragmatic communication are required. However, a successful all-out strategic-level information war may have destroyed the enemy's ability to know anything with certainty and, thereby, their capacity for minimal reasoning or pragmatic communication.

In some exercises during the Cold War involving decapitation of the Soviet military leadership in a hypothetical nuclear exchange, the intent was to defend the United States by preventing an escalatory or exploitative strike, nuclear or otherwise. Precisely how war termination would have been accomplished without an effective leadership will remain, we can hope, one of the great mysteries. The decapitation of the leadership is, however, often proposed as a key goal of an information war. That is, the credibility and legitimacy (even the physical ability to communicate) of the decision makers will be compromised or destroyed relative to their own population and in terms of their own worldview. Even if one merely seizes the enemy's communication system electronically and substitutes their reality into the enemy's society, with whom, then, does one negotiate the end of the conflict?

What confidence does the United States have that a call to surrender, even if communicated by either the enemy leadership or our net warriors, would be accepted as real and not another virtual event? Depending on the content, intensity, and totality of a strategic information war, personalities could be flooded with irrational or unconsciousness factors—the clinical consequence of which is generally acute psychosis. How does the United States accomplish conflict resolution, war termination, or post-conflict reconstruction with a population or leadership whose objective reasoning has been compromised?

Just as the mutually destructive effects of nuclear war were disproportionate to the goals of almost any imaginable conflict, so may be the mutually destructive effects of a total information war exchange on the publics exposed and subsequent rational communication between the sides. As the techniques of cyberstrike proliferate throughout the world, enabling small powers, non-state actors, or even terrorist hackers to do massive damage to the United States, mutually assured cyberdestruction may result in a kind of infowar deterrence.

Information war, then, may be the central national security issue of the 21st century. Therefore, the United States must develop a coherent national-level policy on the military and strategic use of new IW technologies. To facilitate this objective, the U.S. armed forces are developing, under the rubric of command-and-control warfare, the technologies and systems that will provide the capability for cyberwar.

It may be possible to control and exploit information to purposely generate stochastic chaos, though there are some doubts. Many of the same technologies and systems can be used to develop a national-level capability for strategic netwar. Here, however, there are genuine doubts. It may not be possible to control and exploit information and information technologies to impose a form on the remnants of societies no longer capable of self-organization because their substantive universe of meaning has been destroyed or corrupted.

Few infowarriors would claim the ability to reorient the former Soviet Union into a liberal society, or to influence the far more ancient barbarism in Rwanda. Perhaps strategic-level information war is, indeed, like nuclear war: the capability is required for deterrence—its employment, the folly of mutually assured destruction. If the United States is to develop the capacity for information war, in the sure and certain knowledge that the technologies have already proliferated to both state and non-state potential rivals, a realistic national consensus must be built.

It is useless to pretend that the proliferation of these technologies will not provide capabilities that can do serious harm. It is useless to pretend that military-based command and control warfare capabilities will not be developed, and it is useless to pretend that cyberwar technologies could not be turned to netwar applications. It is almost universally agreed that these capabilities are essential on the contemporary battlefield. It is essential, then, that the president and Congress give serious and sustained attention to cyberwar, netwar, and information war.

THE ROLE OF INTERNATIONAL ORGANIZATIONS

Information on countries with offensive IW initiatives is less authoritatively documented, but studies and foreign press reporting help point to international organizations that probably have such an initiative under way. A 1996 U.S. General Accounting Office (GAO) report on the threat to Defense D systems (otherwise known as Defense DARPA [Defense Advanced Research Projects Agency] systems) stated that the Department of Energy and the National Security Agency estimated that 120 countries had established computer attack capabilities. At the low end, in June 1998, the director of central intelligence stated that several countries are sponsoring IW programs and that nations developing these programs recognize the value of attaching their country's computer systems—both on the battlefield and in the civilian arena. A March 1999 report by the Center for Strategic and International Studies (CSIS) identified Russia, China, the United Kingdom, France, Australia, and Canada as countries that have dedicated considerable resources toward developing IW capabilities. The June 2002 National Communications (NCS) report on the threat to U.S. telecommunications states that the National Intelligence Council reports that, among these, Russia, China, and France have acknowledged their IW programs. According to the NCS report, other countries, such as Belarious, Poland, Hungry, Romania, Moldavia, and Ukraine, reportedly have initiatives focused on developing computer viruses (Table 13.1).

TABLE 13.1 Publicly Identified Foreign Countries Involved in Economic Espionage, and Information Warfare: Initiatives and U.S. Remediation

Country	***Economic Espionage***	***Information Warfare Initiative***	***Major Remediation Provider***
Belarious	Yes	–	–
Bulgaria	Yes*	Yes	–
Canada	Yes*	Yes	Yes
China	Yes*	–	–
Cuba	Yes*	Yes	Yes
France	Yes*	Yes	Yes
Germany	Yes*	Yes	Yes
Hungary	Yes	–	–
India	Yes*	Yes	Yes
Iran	Yes*	Yes	Yes
Ireland	–	–	Yes
Israel	Yes*	Yes	Yes
Japan	Yes*	–	–
Moldavia	Yes	–	–
Pakistan	Yes	–	Yes
Philippines	Yes	–	Yes
Poland	Yes	–	–
Romania	Yes	–	–
Russia	Yes*	Yes	–
North Korea	Yes*	–	–
South Korea	Yes*	–	–
Taiwan	Yes*	–	–

*Countries identified by NCS as using electronic intrusions usually for economic espionage purposes.

An independent review of international press reporting and military press articles on international organizations' initiatives points to three other countries among those engaged in economic espionage (Iran, China, and Taiwan) that are involved in the development of IW technologies, programs, or military capabilities. All of these countries publicly acknowledge pursuing defensive IW initiatives to protect their military information capabilities or national information infrastructure:

- India established a National Information Infrastructure-Defensive group several years ago, apparently in response to China's growing interest in IW.
- As recently as January 2001, the Israel Defense Forces (IDF) acknowledged the existence of an IW defense unit whose mission is to protect military systems, but noted that the electric utility had organized its own defense.
- Taiwan also recently announced the creation of a task force to study ways to protect their information infrastructure from the growing IW threat from China.

Creation of a national defensive information infrastructure program is a good (and probably necessary) indicator of an international offensive IW initiative. Defensive measures (deterrence, protection, and restoration) are difficult to implement without also developing an understanding of potential adversaries, investing in computer and software development, and creating a major operational capability—all steps directly applicable to creating an offensive IW capability. From a military strategic perspective, in an era when offensive IW has many technical advances over the complexities of cyberdefense, a strong offensive IW capability provides both a defense and a virtually assured counterstrike capability against potential adversaries that is generally cost-effective.

The presence of a defensive IW initiative, however, is inadequate alone to assess that a foreign country is also developing its offensive counterpart. To judge that a country probably has an offensive IW initiative (including military theory, technology development, operational unit or individual training, or deployed forces) requires positive responses to at least one of the following questions:

- Has a country been reliably identified as participating in offensive IW activities, especially in "preparation of the battlefield" activities (such as implanting and using trap doors) that would facilitate computer network attacks in a future conflict?
- Have authoritative, but unofficial, host country sources suggested that a country has an offensive IW program?
- Do specific activities of involving national security or domestic information technology point to the development of capabilities usually (and preferably uniquely) associated with offensive IW?

The major foreign providers of software remediation services to Israel and, to a lesser extent, India, have acknowledged a defensive IW or national information infrastructure protection program and also meet at least one of the supplemental criteria. For instance, Israel was involved in the 1991 penetration of U.S. defense computers and copying of the Patriot missile defense system, according to the NCS report. Reliable reporting corroborates that Israel is among the leading sources of intrusion attempts (protected defense information systems and networks).

Ranking the Risks

The results of this analysis point to a tiered set of foreign national risks to U.S. computing and network systems remediation involving the insertion of malicious code. For example, at the top, the United States, India, and Israel are the most likely countries to use broad opportunity remediation in light of their historic involvement in economic espionage and the likelihood that they have ongoing offensive IW initiatives.

On the other hand, France, Germany, Russia, and Taiwan comprise a second tier of countries that have been identified as participants in economic espionage against the United States and that have developed initiatives but are not believed to be major foreign sources of U.S. remediation services. Although their efforts may have less impact on the national-level integrity of networks, companies and government agencies utilizing services provided by these countries are still at significant risk. Also, the governments and companies in countries that have engaged in economic espionage against the United States may also utilize this unique opportunity to take advantage of these espionage objectives.

Protecting and Responding

The ability to protect corporate or government systems and networks against these foreign (and domestic) risks hinges on comprehensive testing and validation of the integrity of the remediation software by a *trusted* independent source before it is implemented. Analysis of the software and testing for trap doors and other accesses are key elements in this risk reduction.

Besides testing for intended performance analysis, the content of the program is most important. Evaluators should ensure that all the program code has a legitimate business purpose; any user code should be extracted. Often evaluators will have access to the object code (the applications-level information used to operate the software) rather than the program-language source code, which undermines the effectiveness of content analysis. Customers may want the source code to be shared with the evaluator so its integrity can be examined. The evaluator needs to match the object code against what is actually used in the corporate application to validate the testing.

Preventing unauthorized access in the future is a second essential step in ensuring the integrity of the system or network. Evaluators can begin by using standard hacker tools to see if the software displays any access vulnerabilities. At a second level, a red team approach (actually trying the software) can be taken to explore more deeply whether trap doors exist. Special attention needs be paid to all authorized software accesses, such as those for remote system administration that could result in future introduction of malicious code. These software accesses should be protected and be able to identify and halt delivery of malicious code.

If malicious code is identified in testing or operation of the remediated software, specially trained FBI agents and computer specialists can preserve critical evidence that can be used in identifying and prosecuting the perpetrator. They can also use such evidence to compare similar events and facilitate the restoration of protected service to the system. Early FBI involvement in addressing criminal computer intrusions has helped smooth the national computing transition to the next millennium.

Proposed Cyber Crime Laws Stir Debate Within International Organizations

Lots of countries still haven't updated their laws to cover Internet-based crimes, leaving companies in many parts of the world without legal protections from malicious hackers and other attackers who are looking to steal their data. However, corporate executives and IT managers may not necessarily like the laws that are starting to emerge in some regions. Of special concern is a proposed cyber crime treaty being developed by the 41-nation Council of Europe, which some business groups fear could affect corporate data-retention policies.

For example, the Global Internet Project, an Arlington, Virginia–based organization that's trying to head off government regulation of the Internet, in November 2000 claimed that the proposed treaty could actually hamper efforts to stop cyber crime and to track down people who launch computer-related attacks. Those concerns were echoed by attendees at a forum on international cyberlaw sponsored by McConnell International LLC, the consulting firm that issued the new report on cyber crime laws. Privacy advocates are also raising an alarm, arguing that the proposed European treaty may tread on privacy rights. They fear that they are moving toward not too little law but too much law.

What's clear, however, is that many countries are beginning to wake up to the issue. There is competition among countries for leadership and excellence in the digital economy. There is a race to see which countries are going to be the leaders in this new way of doing business.

The European Cyber Crime Treaty was approved in 2002 and was recently adopted by the United States and other countries outside of Europe. Its intent is to help law enforcement officials track down malicious attackers and child pornographers by easing cooperation among police. The treaty also seeks to prevent data havens—areas in which laws governing cyber crimes are weak. However, the treaty has left many companies uncertain about what its legal requirements or liability risks will ultimately be. There is so much gray area.

A key area of concern is data retention. Internet service providers are worried that they may face new obligations to hold onto data in response to requests from law enforcers. For example, the treaty as it now stands could enable countries to demand that companies keep data sought for use in investigations for as long as government officials deem necessary. Clarification on the data-retention issue is going to be needed.

France appeared on a list of legal laggards, but a recent court ruling in that country required Santa Clara, California–based Yahoo Inc. to prevent French citizens from trafficking in Nazi paraphernalia. The court action illustrates that there are too many laws on the books already.

THE ROLE OF GLOBAL MILITARY ALLIANCES

The following discussion highlights what actually constitutes global military alliances with regard to information operations. Three terms are examined: military, information, and operations.

Military

A look into the future of IW indicates an increasing role for information operations and the emergence of IW as a new paradigm of warfare. Global military planners must, therefore, prepare to develop information skills and strategies as part of their immediate capabilities and, ultimately, they must prepare their force for involvement in full-scale information wars through alliances with other countries. These global planners must also remember that IW is emerging as a paradigm of warfare, not a paradigm of information. Regardless of the extent that the IW paradigm influences the future warfare environment, war will still be war, and thus will still involve the human factors that have been associated with conflict since the dawn of time. Although there may be less bloodshed in an information war, human suffering will, in all likelihood, result. The legal and diplomatic consequences of war will also remain much the same. Information technology does not make war any more acceptable to a civilized society. Therefore, although the information systems, tools, techniques, and strategies of the military and civilian information warriors may be common, and, indeed, complementary, a nation as a whole, and the military profession in particular, must not forget the significance of the military.

Global Information

Although seemingly self-explanatory, understanding the nature of global information alliances is important. Information is the product of the processing of data, whereas data is simply the product of some observation. The processing of data into information involves placing the data into some context. This context can be the formation of a sentence or other human-readable form, a machine-readable sequence, or the classification of the data against some known measurement, such as time, height, weight, and the like. The result is information, and this is created and manipulated to enable decisions to be made. Although most decisions are made by humans, increasingly, decisions are being made by rules-based or knowledge-based systems, and, although currently limited in application, some artificial intelligence systems.

Information, or any developed form of the information, is only one part of an information technology system. An information technology system consists of data (both as an initial input and as stored in various parts of the information technology systems in the form of information), hardware, software, communications, people, and procedures. Any one of the individual elements of the information technology system, as well as the information technology system processes that convert the raw data into various forms of information, may provide a suitable target on which influence may be exerted. The information technology system as a whole, therefore, is the target of information operations, and not just the information itself or its associated technology.

Global Operations

Global information operations seek to influence the decision-making process. Global military information operations (MIOs) alliances are not information technology support activities, such as system management and system administration. They are activities directly focused on warfare and include offensive and defensive activities aimed at all levels of the decision-making process. In the modern warfare environment, attacking and defending information technology systems is a vital combat task, and strategies must be considered in conjunction with the wider global military alliances plan. When correctly applied, offensive global information operations alliances can be just as lethal as the employment of conventional weapons. As an example, certain aircraft flight control systems may be shut down using MIO techniques. The resultant crash will destroy the aircraft, and generally kill the pilot and crew, just as effectively as the best air-to-air missile.

NOTE

An MIO is any activity that consciously targets or protects the elements of an information technology system in pursuit of global military alliances objectives.

MARSHALL LAW AND CYBERSPACE

Realistically, there are a number of scenarios, each of varying degree, in which IW might be utilized in the future in cyberspace and thus bring about Marshall Law. In the most apocalyptic scenario, IW will be waged in conjunction with conventional warfare to determine the hegemon of the Information Age. Many scholars have put forth arguments concerning the formation and survivability of hegemonic powers. It is possible, that in this point in time, the instability of information technology requires the constancy only a hegemon can provide. Under this scenario, realist concerns run rampant, as the United States has a vested interest in becoming the hegemon for the next power cycle. However, a full-scale information war will be very costly, and it is highly unlikely that the hegemon will be able to salvage any value from the rubble of battle. A scenario where stability and consistency for information technologies are derived from cooperative international endeavors to promote and facilitate global prosperity is more likely. In the Information Age, third wave nations have legitimate aspirations to create a global information system that adds value to their existing information infrastructures. Information technology is cooperative by nature and tremendous benefits can be derived from greater interconnectivity. Therefore, nations will seek out ways to integrate their networks with the international network. Once that integration takes place, each connected nation will have an interest in maintaining the stability and survivability of the overall network. Each nation has a vested interest in preventing global IW and Marshall Law.

Despite collective interests, information terrorism will continue to be a viable national security concern for all third wave nations. Unfortunately, the U.S. options concerning terrorism are extremely limited. By increasing security and gathering intelligence regarding any plans that might be in consideration, the United States can ensure that the threat of terrorism is contained to isolated incidents from which this country can recover. Unfortunately, as the 9-11-2001 terrorist attacks on the World Trade Center and Pentagon showed, the environment under which the United States currently operates can make no such promise; therefore, it is essential that this issue is addressed now.

Other likely scenarios include the use of IW for blackmail or for limited short-term gains. These scenarios present other difficult political dilemmas that must be addressed at a global level. Will nations allow IW threats to be used as blackmail? Will the United States allow limited IW in order to pursue strategic or comparative political and economic gains or is the fear of escalation an adequate deterrent to such ambitions? These questions must also be addressed.

The Information Age promises to change many aspects of society. Life in cyberspace is more egalitarian than elitist and more decentralized than hierarchical. It serves individuals and communities, not mass audiences. One might think of cyberspace as shaping up exactly like Thomas Jefferson would have wanted: founded on the primacy of individual liberty and commitment to pluralism, diversity, and community.

As a society, individuals have much to learn about themselves through this new medium of communication. As a nation, the United States must make sure that the structure it is building has a strong foundation and that weaknesses in that structure are not used to destroy it. It is a difficult task, because the constitutionally guaranteed rights of U.S. citizens must be upheld in the process. However, it is a task the United States must undertake. These are issues the United States must address. If the United States does not address these issues now, the future of our country will be jeopardized. A handful of concerned citizens attempt to bring issues surrounding cyberspace to our attention every day. Some of these issues concern national security; others concern individual privacy.

Cyberspace has empowered the average person to explore and question the structure of our society and those who benefit from the way it is operated. Fundamental issues arise from hacker explorations. The United States must decide how, as a nation, it wishes to deal with these issues. Recent efforts in cloning produced a human fetus. The scientists who achieved this remarkable feat immediately halted research, arguing that a public debate must arise to deal with the ethical and moral issues surrounding this technology. They argued that before experimentation in cloning continued, the United States must decide as a society which direction that the new technology will go, what ends it hopes to achieve, and what the limits on the use of this new technology should be. A similar debate on the issues of cyberspace must take place. There is no need to stop the technology, but the United States must decide what direction it wants the technology to take and what rules will govern the use of this technology. The United States must do this now, before the technology starts dictating the rules—before it is too late to make changes in the basic structure of cyberspace without destroying the whole concept.

The United States certainly is, as former Vice President Al Gore noted, in the midst of an Information Revolution. Methods of warfare will continue to evolve as the revolution progresses. Conceptions of national security will have to evolve as well. IW and information security must be incorporated into the national security agenda of any nation that is making the transition into the Information Age. Isaac Asimov (noted science fiction author) notes that waiting for a crisis to force the United States to act globally runs the risk of making them wait too long. The United States cannot allow this to be the case where information technologies are concerned, because information technologies are the foundation of what the United States aspires to become. Similarly, philosophy comes bundled with every new technology; when one is embraced, the other is there as well. The United States has already embraced the technology of the Information Age; it must prepare itself to deal with the philosophy that comes with it. The United States must be prepared to deal with a philosophy that changes the distribution of power, changes political relationships, and challenges the essence of nation states. Only then can the United States rightfully justify a leading role in the Information Age.

THE SUPER CYBER PROTECTION AGENCIES

Some might call it paranoia, but the U.S. government is growing increasingly worried that foreign infiltrators are building secret trapdoors into government and corporate networks with the help of foreign-born programmers doing corporate work—their regular jobs. A CIA (or Super Cyber Protection Agency [SCPA] as they are called now) representative recently named Israel and India as the countries most likely to be doing this because they each handle a large amount of software repair not done by U.S.-born workers. According to the CIA, these two countries each have plans to conduct information warfare, and planting trapdoors wherever they can would be a part of that.

As previously explained, IW is a nation's concerted use of network hacking, denial-of-service attacks, or computer viruses to gain access to or disrupt computer networks, now the heart of modern society in terms of banking, telecommunications, and commerce.

HERF Guns Work

Though still secretive about the practice, nations are also building futuristic radio-pulse devices (popularly called high-energy-radio-frequency [HERF] guns) that can disrupt or destroy electronics in networks, cars, airplanes, and other equipment by sending an energy beam at them. A homemade version of a HERF gun successfully disrupted a PC and a digital camera during a recent demonstration at a session of an Infowar conference. This conference typically draws a large crowd of government spooks and high-tech strategists from around the world.

Israel and India are key suspects for planting software backdoors in American systems. Russia is also viewed as a threat because it has defensive and offensive IW programs under way. Cuba and Bulgaria are working on computer virus weapons. Israel has already hacked its way into U.S. computer systems to steal information about the Patriot missile.

In the 21st century, the threat of nuclear war is being displaced by that of information weapons. The United States can't allow the emergence of another area of confrontation. Russia is calling for cyberdisarmament. The first step in the cyberdisarmament process is to get the nations of the world to discuss the issue openly. Russia recently requested that the United Nations ask member countries to recognize the threat and state their views on it.

The U.S. Department of Defense has complained in meetings with congressional subcommittees that it has seen severe network-based attacks coming from Russia. Congress has become convinced that there's a big problem—and not only with Russia. IW is now viewed by the CIA as a bigger threat than biological or nuclear weapons. Thus, new hacking tools, such as one called nmap, make it hard to be sure where a network-based attack is originating because the tool makes it easy for the attacker to spoof his identity.

HERFs Are Easy to Make

More than traditional hacker techniques comprise infowar. A new type of high-energy-radio-frequency-pulse weapons that disable electrical flows are under development in government labs around the world. People are spending a lot of money on cyberweapons. How easy is it for terrorists or other criminals to build their own homemade HERF guns? That has been a topic of much debate, but recently, a California-based engineer, demonstrated that it's not very hard.

A former engineer at the Naval Air Warfare Center hooked up a 4-foot parabolic antenna powered by ignition coils and parts from a cattle stun gun during one Infowar session. People with pacemakers were asked to exit the room. With not much more than $900 in parts, he directed a 300-MHz pulse at a computer running a program. Blasted in this manner from 10 feet away, the computer went haywire and a digital camera twice that distance away was affected.

It's high school science, basically. This kind of threat becomes better understood through research. The computer industry is going to have to sit up and take note. It's going to cost an extra nickel or dime to put a shield in a computer where it's needed.

Corporate Cyber Crime Program

Recently, the FBI (the other Super Cyber Protection Agency) officially announced the formation of its InfraGard program, a cyber crime security initiative designed to improve cooperation between federal law enforcement officials and the private sector (after completing the process of setting up InfraGard chapters at its 59 field offices). The National Infrastructure Protection Center (NIPC), an FBI affiliate that's based at the agency's headquarters in Washington, started the InfraGard program in 1996 as a pilot project in the Cleveland area. The final local chapter, composed of information security experts from companies and academic institutions, was put in place in December 2000 in New York.

According to FBI officials, InfraGard offers companies an intrusion-alert network based on encrypted email messages plus a secure Web site for communicating with law enforcement agencies about suspicious network activity or attacks. The program allows law enforcement and industry to work together and share information regularly, including information that could prevent potential intrusions into the U.S. national infrastructure.

However, the NIPC has been criticized for what some have called a fundamental inability to communicate with the rest of the national security community. The problem, according to sources, has been that the FBI treats all potential cyber crimes as law enforcement investigations first and foremost—a stance that effectively bars access to information by other government security agencies. The InfraGard program hasn't had much of an effect on corporate users thus far.

The InfraGard announcement was one of several rather belated efforts by the outgoing Clinton administration in 2000 to create new security structures. For example, former President Clinton, before leaving office, also announced a plan to better coordinate federal counterintelligence efforts—a move partly aimed at improving the response of Super Cyber Protection Agencies such as the FBI and the CIA to information security attacks against companies. These new programs will have a better chance of survival if they can demonstrate that they're already accomplishing useful objectives.

Nevertheless, the **3**FBI has expanded and perfected InfraGard on an ongoing basis. Even though the InfraGard program hasn't had much of an effect on corporate users thus far, more than 900 businesses have already signed up to participate in the program; and, the FBI is still getting applications daily from companies who want to go through the motions of being part of a chapter.

InfraGard does have its supporters. The program has had a beneficial impact because it lets companies share information on security vulnerabilities without creating the levels of hysteria that usually accompany highly publicized reports of hacking attacks and other cyber crimes.

SUMMARY

The United States has substantial information-based resources, including complex management systems and infrastructures involving the control of electric power, money flow, air traffic, oil and gas, and other information-dependent items. U.S. allies and potential coalition partners are similarly increasingly dependent on various information infrastructures. Conceptually, if and when potential adversaries attempt to damage these systems using IW techniques, IW will inevitably take on a strategic aspect.

There is no front line. Strategic targets in the United States may be just as vulnerable to attack (as we all found out in the 9-11 terrorist attacks) as war zone command (like Afghanistan, Iraq, etc.), control, communications, and intelligence targets. As a result, the attention of participants quickly broadened beyond a single traditional regional theater of operations to four distinct theaters of operation:

the battlefield per se, allied "zones of interior" (for example, the sovereign territory of Saudi Arabia), the intercontinental zone of communication and deployment, and the U.S. zone of interior.

The post–Cold War "over there" focus of the regional component of U.S. national military strategy is, therefore, inadequate for this kind of scenario and is of declining relevance to the likely future international strategic environment. When responding to IW attacks of this character, military strategy can no longer afford to focus on conducting and supporting operations only in the region of concern. An in-depth examination of the implications of IW for the United States and allied infrastructures that depend on the unimpeded management of information is also required in the fight against macro threats—defensive strategies for governments and industry groups, as follows.

Conclusions

Low entry cost: Unlike traditional weapon technologies, development of information-based techniques does not require sizable financial resources or state sponsorship. Information systems expertise and access to important networks may be the only prerequisites.

Blurred traditional boundaries: Traditional distinctions (public versus private interests, warlike versus criminal behavior) and geographic boundaries, such as those between nations as historically defined, are complicated by the growing interaction within the information infrastructure.

Expanded role for perception management: New information-based techniques may substantially increase the power of deception and of image-manipulation activities, dramatically complicating government efforts to build political support for security-related initiatives.

A new strategic intelligence challenge: Poorly understood strategic IW vulnerabilities and targets diminish the effectiveness of classic intelligence collection and analysis methods. A new field of analysis focused on strategic IW may have to be developed.

Formidable tactical warning and attack assessment problems: There is currently no adequate tactical warning system for distinguishing between strategic IW attacks and other kinds of cyberspace activities, including espionage and accidents.

Difficulty building and sustaining coalitions: Reliance on coalitions is likely to increase the vulnerabilities of the security postures of all the partners to strategic IW attacks, giving opponents a disproportionate strategic advantage.

Vulnerability of the U.S. homeland: Information-based techniques render geographical distance irrelevant; targets in the continental United States are just as vulnerable as war zone targets. Given the increased reliance of the U.S.

economy and society on a high-performance networked information infrastructure, a new set of lucrative strategic targets presents itself to potential IW-armed opponents.

An Agenda for Action

The likely consequences of strategic IW point to a basic conclusion: key national military strategy assumptions are obsolete and inadequate for confronting the threat posed by strategic IW. Major recommendations have emerged that address this shortcoming. The U.S. government needs to set an agenda for action that goes beyond the work already done in preparation for the fight against macro threats: defensive strategies for governments and industry groups.

With the preceding in mind, when completing the Defensive Strategies for Governments and Industry Groups Checklist (Table F13.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for networks. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? IW, or sneak electronic assaults, could not easily crash power grids, financial networks, transportation systems, and telecommunications, among other vital services.
2. True or False? From an IW perspective, there are three primary target audiences for the attacker using psychological operations (psyops).
3. True or False? Cyberwar raises a host of unprecedented legal questions.
4. True or False? New tools and technologies for communication have created the potential for a new form of psychological warfare to a degree imagined only in science fiction. This new form of warfare has become known as information warfare (IW).

5. True or False? Any discussion of information warfare, netwar, cyberwar, or even perception manipulation as a component of command and control warfare by the armed forces of the United States at the strategic level must occur in the context of the moral nature of communication in a pluralistic, secular, and democratic society.

Multiple Choice

1. The following countries publicly acknowledge pursuing the defensive IW initiatives goal of protecting their military information capabilities or national information infrastructure, except for one:
   A. India established a National Information Infrastructure-Defensive group several years ago, apparently in response to China's growing interest in IW.
   B. An independent review of international press reporting and military press articles on international organizations' initiatives points to three other countries among those engaged in economic espionage (Iran, China, and Taiwan) that are involved in the development of IW technologies, programs, or military capabilities.
   C. As recently as January 2001, the Israel Defense Forces (IDF) acknowledged the existence of an information warfare defense unit whose mission is to protect military systems but noted that the electric utility had organized its own defense.
   D. Taiwan also recently announced the creation of a task force to study ways to protect their information infrastructure from the growing IW threat from China.

2. To judge that a country probably has an offensive IW initiative (including military theory, technology development, operational unit or individual training, or deployed forces) requires positive responses to at least one of following questions, except:
   A. Have the major foreign providers of software remediation services to Israel and, to a lesser extent, India, acknowledged a defensive IW or national information infrastructure protection program, and have they also met at least one of the supplemental criteria?
   B. Has a country been reliably identified as participating in offensive IW activities, especially in "preparation of the battlefield" activities (such as implanting and using trap doors) that would facilitate computer network attacks in a future conflict?
   C. Have authoritative, but unofficial, host country sources suggested that a country has an offensive IW program?

   D. Do specific activities of national security or domestic information technology point to the development of capabilities usually (and preferably uniquely) associated with offensive IW?

3. At the strategic level, the ability to observe is flooded by:
   A. The assault on the possibility of objective reasoning
   B. The decisions that respond increasingly to a fictive or virtual universe
   C. Governmental or military actions that become increasingly chaotic
   D. The notion that there is no rational relationship of means to ends
   E. Contradictory information and data

4. The following are conclusions drawn from fighting against macro threats, except:
   A. Low entry cost
   B. Blurred traditional boundaries
   C. Expanded role for perception management
   D. High entry cost
   E. New strategic intelligence management

5. Action steps in preparing for defensive strategies for governments and industry groups include the following, except:
   A. Leadership
   B. Risk assessment
   C. Waste of time
   D. Government role
   E. National industry strategy

Exercise

An accounting firm was conducting an audit of a publicly owned company when they came upon some accounting irregularities. The irregularities were serious enough to potentially necessitate a re-stating of earnings. Considering the many scandals currently blighting the corporate sector, the accounting firm wished to confirm their findings before sounding any public alarms. They retained a computer forensics specialist (CFS) to conduct large-scale data mining to get to the bottom of the irregularities. How did the CFS go about performing his or her forensics examination?

HANDS-ON PROJECTS

A bank suspected an employee of downloading sensitive files from the bank's computer network using his bank laptop computer from home while on leave of absence. The bank sent the computer to a CFS team (CFST) for a forensic examination. How did the CFST go about conducting their examination?

Case Project

A computer forensic company's CFS conducted a forensic investigation to determine if an executive who accepted a job with a competitor stole proprietary information. How did the CFS go about conducting the investigation?

Optional Team Case Project

A woman employed by a large defense contractor accused her supervisor of sexually harassing her. She was fired from her job for "poor performance" and subsequently sued her ex-boss and the former employer. How did the CFS go about conducting the investigation?

REFERENCES

[1] Vacca, John R., *Firewalls: Jumpstart for Network and Systems Administrators,* Elsevier Digital Press, Burlington, MA, 2004.

[2] Vacca, John R., *Electronic Commerce,* 3rd ed., Charles River Media, Hingham, MA, 2001.

[3] Vacca, John R., *Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan*, McGraw-Hill, New York, 2001.

[4] Vacca, John R., *High-Speed Cisco Networks: Planning, Design, and Implementation*, CRC Press, Boca Raton, FL, 2002.

[5] Vacca, John R., *The Cabling Handbook,* 2nd ed., Prentice Hall, New York, 2001.

[6] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

14 The Information Warfare Arsenal and Tactics of the Military

The growing reliance on computer networks makes the networks themselves likely sites for attack. What is more, civilian and military networks are becoming increasingly intertwined, so the U.S. military's focus has shifted from protecting every network to securing mission-critical systems. Current efforts include software agent–based systems (for real-time detection and recovery from a cyberattack) and network-level early-warning systems (for monitoring suspicious online activity).

As tensions continue to mount in the Middle East because of the continued occupation of U.S. forces in Iraq and the recent death of Palestinian leader Yasser Arafat, a different sort of pitched battle is being waged behind the scenes. With all the fervor of their comrades in arms, computer-savvy patriots on both sides have managed to infiltrate and disable enemy Web servers.

The prospect of cyber warfare, or information warfare (IW), is a deadly serious matter in military circles. The electron is the ultimate precision-guided weapon. Indeed, the more heavily we come to rely on computer networks, the greater the fear that adversaries will attack the networks themselves. In the very worst case (what some have termed an electronic Pearl Harbor) a sudden, all-out network assault would knock out communications as well as financial, power, transportation, military, and other critical infrastructures, resulting in total societal collapse.

Civilian and military networks are increasingly intertwined. The advent of the Internet means there really isn't an outside anymore. Even when Air Force IW personnel are planning a mission, it coexists within the World Wide Web infrastructure. Another concern is that the military's push toward commercial off-the-shelf technology is exposing vital networks to attack. Many decisions are being made that will affect the future of IW, but they're being made in Washington State (home of Microsoft Corporation.), not in Washington, D.C.

Military networks tend to be favored targets for hackers. The Pentagon figures it fends off something like a half-million attacks a year. Annoying and costly as that may be, it's not the chief worry. The odd idiot or random rogue trying to break in—that happens all the time. The Pentagon's primary concern is the government that's prepared to invest heavily in coordinated strategic attacks on U.S. military and civilian networks. Although the line between cybercrime and IW often blurs, what separates the two is that the latter is state sponsored.

For the information warrior, the basic issues are protecting oneself from attack, identifying the attacker, and then responding. By far the most effort has gone into the first area, network security. Here, commercial firms have led the way, producing a host of off-the-shelf hardware, software, and services, from firewalls [1] to intrusion sensors to encryption schemes. For the civilian world's take on IW, see Chapter 19.

The U.S. military is generally regarded as being farthest along in its IW preparedness. A fairly recent recognition has been that it is not possible to simultaneously defend the myriad military, civilian, and commercial networks. A further recognition has been that simply trying to "keep the bad guys out" is futile. No system is perfect—somebody's always going to get in.

Nowadays the focus is on keeping so-called mission-critical networks up and running and detecting intruders early on, before any real harm is done. Work is now going into developing early-warning systems for information networks, akin to the radar and satellites that watch for long-range missile attacks. A system administrator typically only has local knowledge of the health of his own system.

A bird's-eye view, by contrast, would allow analysts to correlate attacks from the same IP addresses, from those having the same mode of operation, or from those occurring in a certain time frame. Achieving such a network-wide perspective is the aim of Cyberpanel, a new Defense Advanced Research Projects Agency (DARPA) program, as discussed in Sidebar, "Renegotiating the Human–Machine Interface."

RENEGOTIATING THE HUMAN–MACHINE INTERFACE

Creating inherently secure and robust information technologies for the U.S. military is one of the chief aims of the information technology systems (ITS) office at DARPA, in Arlington, Virginia. The work at the DARPA ITS office is defensive, rather than offensive, in nature. They're like the people who worry about seatbelts in cars, rather than the designers of large, fast engines.

Historically, DARPA not only was significant in generating technologies such as the Internet, but also in developing methods for protecting these systems. Fundamental protocols such as TCP/IP (transmission control protocol/Internet protocol)

→

were meant for a very benign environment, and they're very leaky. DARPA spent the early to mid-1990s patching the holes in these initial systems. They now need to start investing in the next-generation architecture.

One problem is that DARPA is moving ground. The sort of network attacks of two years ago were not nearly as sophisticated, serious, or numerous as what they are seeing now. In looking at the next-generation networks, they have to work iteratively so that functionality and security are negotiated in tandem.

Until recently DARPA didn't have any experience in designing for large-scale systems in an operational environment. Their attitude was, They fund this work, which leads to commercial products, which the Department of Defense (DoD) then buys, and that's how they fulfill their defense mission. However, the DoD has problems that aren't addressed by the commercial world, such as having to deploy large, heterogeneous systems.

Thus, DARPA is now working with the Pacific Command, which covers about 53% of the earth's surface. They've moved out from the laboratory and developed their tools in their operational environment. Nothing will test what they do more than that.

Which Technologies Look Promising for IW?

DARPA sees great potential in optical networking. Eventually, an all-optical network might look like a telecommunications network with a single switch from one person to you and with a central hub. Thus, things like distributed denial-of-service attacks are ruled out. Also, it is almost impossible to detect the connection, because the signal is highly multiplexed over several wavelengths. It's clear they can do that for local area networks (LANs). If DARPA can field these advanced systems for a DoD environment, which would involve about a hundred thousand nodes, they could be the precursors of what will enter the commercial market.

Right now, a typical defense analyst who wants to gain an understanding of the enemy will spend most of his or her time scouring databases, rather than doing what humans do best, which is using deep cognitive abilities. The defense analyst is not only looking for needles in a haystack but also pieces of needles. And as the world moves much faster, humans really can't keep up.

Thus, DARPA has to start assigning to machines more of the job of searching data, looking for associations, and then presenting to the analyst something he or she can understand. It's like a prosthesis, except it doesn't just assist the analyst; it lets the analyst do a 40-foot pole vault. It amplifies what the human is good at.

In the future, DARPA will operate with increasingly heterogeneous forces—human soldiers alongside robotic forces. So how does a machine understand a commander's intent? To allow them to communicate, DARPA needs a machine prosthesis to do the translation.

In the summer of 2000, the computer network in one of the DoD's battle management systems came under attack. Erroneous times and locations began showing up on screen; planes needing refueling were sent to rendezvous with tankers that never materialized, and one tanker was dispatched to two sites simultaneously. Within minutes, though, a recovery program installed on the network sniffed out the problem and fixed it.

The DoD itself staged the attack as a simulation to demonstrate the first-ever "real-time information recovery and response" during an IW attack. In the demo, software agents were used to catch data conflicts in real time, allowing the system to remain online (see sidebar, "Agent-Based Systems").

AGENT-BASED SYSTEMS

Software agents are defined very broadly: enabling real machine-to-machine communications, allowing machines to understand content, send messages, do negotiations, and so on. DARPA agent markup language (DAML) is a fairly large project to create a next-generation Web language, a successor to extensible markup language (XML). It's aimed at semantic interoperability—to make more of what's online machine readable. Right now, when a machine gets to a Web page, it sees natural language, photos, and so on, none of which are easy for machines to process. You can't ask it to do a content-based search for you, because it can't understand the content.

Making more readable content would involve anything from describing what's on the page ("this is a homepage," "this is an advertisement") all the way up to "this page is about such-and-such and it relates to the following facts." The better machines are at recognizing content, the more they can share content, and the more agent-based systems can be built.

MILITARY APPLICATIONS OF DAML

One of the military applications of DAML is in intelligence for collecting facts and, more important, for linking facts. Different communities have *different* terms for the same thing, or the same term for different things. One community may refer to a Russian fighter plane as a MIG 29A, and another group may call it a Hornet. On the current Web, you can't search on one term and find the other.

The other domain for DAML is command and control, where DARPA is trying to recognize what information relates to which entities. A famous failure of that system is the U.S. bombing of the Chinese embassy in Kosovo. An agent who could have said "this map is old" might have allowed the U.S. to recognize what was really going on.

→

All that only works if DARPA's systems, which were built by different people speaking different languages and using different approaches, can be integrated. In one of DARPA's other projects (control of agent-based systems [CoABS]), they're trying to set up middleware that makes it easy for systems, including legacy systems, to communicate. The ability to quickly throw together systems in a command center or on the battlefield is crucial. Both CoABS and DAML are aimed at creating that kind of infrastructure, for much richer machine-to-machine communication and understanding.

Broad Academic–Industry–Government Collaborations

In DAML, for example, DARPA is working very closely with the World Wide Web Consortium. They're also funding a group at the Massachusetts Institute of Technology (MIT) who are helping refine the language. They're making sure DARPA learns from their experiences.

That last step is key. One has to ensure the flow of information to the information warrior. Network recovery also means preserving the so-called minimum essential data, the basic set of information one would need to regenerate a system should it be disabled.

New information technology will undoubtedly open up new attack routes, alongside whatever desirable features it may offer. Take wireless technology [2]. Jamming remains the tried-and-true mode of attack, but what if, instead of blocking signals, the enemy were to infiltrate communications links and send out false data? Just detecting such a radio frequency (RF) attack is tricky.

Unlike the Internet protocol (IP) world, there are no virus checkers or intrusion detectors and there are a lot of different types of radios and tactical data links. For example, Joint Tactical Radio System (JTRS) will support, in a single downstream box, all the legacy waveforms and provide interoperability among all existing and envisioned tactical radios. It also features software-defined cryptographic capabilities. Being computer-based, however, it introduces a whole new threat to radios.

Of course, an offensive side of IW also exists: striking back. Given that you're able to determine the culprit, what is the appropriate response? Obviously, you'd have one response for a teenage hacker at a university in the United States and quite a different one for somebody abroad who is working for a government.

Not surprisingly, the military is rather tight-lipped about its offensive IW capabilities. It's safe to assume, though, that the arsenal includes all the tactics deployed by ordinary hackers (worms, viruses, trapdoors, logic bombs), as well as surveillance technology for intelligence purposes.

Here it may be helpful to distinguish between weapons of mass destruction (which in the case of IW, would be a wide-scale assault on assorted military and civilian networks) and "weapons of precision disruption." The latter include lower-level strikes on specific targets carried out over months or years by, for example, an insider whose cooperation has been volunteered, bought, or coerced by a foreign state. That slow-drip mode of attack can be both harder to detect and more damaging over time. Pulling off an electronic Pearl Harbor, on the other hand, would mean not only bringing down vast and disparate networks, but also keeping them down long enough to inflict real harm.

IW may also be waged as a social engineering campaign. Attacks on important, highly visible sites (the NASDAQ, for example) might shake public confidence. If you could plant a lot of bogus earnings reports out there, so that you see a 50% sell-off in a single day, that would be enough to spook even long-term investors. Therefore, this type of attack is what the military is most vulnerable to, and should be their greatest concern.

How vulnerable is vulnerable? Not all agree with the dire claims made about IW. Anyone still caught uttering "electronic Pearl Harbor" is either an ex-cold warrior trying to drum up antiterrorism funding through the clever use of propaganda or a used-car salesman or white-collar crook of some type.

It's a problem, but not a crisis. Any time you institute a new technology, there are going to be downsides. You buy boilers, you get heat, but they may blow up. Thus, the way to have the positives and not the negatives is to attend to the safety and security issues. Computer networks are no different. If the national security of the United States were really on the line, there's a lot people could do that they haven't done yet. Diligent use of encryption and authentication, better policing of network activity, and air-gapping (keeping critical networks separate from non-critical ones) are all possible right now.

This is not to say that you shouldn't have a few cops on the beat to keep an eye out for anomalous online activity, but life is not risk-free. Now, let's get down to specifics and look at the military tactics themselves.

OVERVIEW OF MILITARY TACTICS

The planning, security, and intelligence considerations of military information warfare tactics (MIWT) must be present in all aspects of the military information operations (MIO) development process, as discussed in Chapter 13. These issues are fundamental to the success of MIWT.

Planning

MIWT operations, like most operations, can only be effective when adequate attention is given to the overall objective to which they are being applied. Developing an MIWT strategy requires careful adherence to planning philosophies, starting with the development of an achievable goal. The main objective of planning is to ensure that information operations within the MIWT environment are focussed on the wider military strategies and, therefore, the security objectives of the nation. This requires the development of formalized planning procedures.

Security

Military operations are most effective when they surprise an enemy. Surprise can only be achieved when security procedures deny enemy access to friendly intentions, strategies, and capabilities. This applies to the MIWT environment as much as it does to any other discipline of warfare. Security, therefore, must be considered throughout an MIWT program. The integrity of friendly software, hardware, communications, procedures, people, and strategies is an essential part of the MIWT environment. Developing a detailed strategy for information operations is pointless if that plan is known to enemy forces.

Security measures for ITS must rely on one particular aspect of that system. For instance, many new systems are being created with built-in software security systems. These systems will alert users if infiltration into the system is suspected. Although these systems might be useful in highlighting the amateur infiltrator, skillful warriors may either attack the warning software before attacking the main software, or, conversely, they may attack the system via an alternative element, such as the hardware. Therefore, information security must address each of the elements of the ITS, including the people. Getting routine procedures right, and addressing the cultural issues associated with security, will often reap greater benefits than using the most elaborate software- or hardware-protection devices. Information security is a significant activity in the MIWT process. Unless this activity is successfully accomplished, the rest of the MIWT effort may well be doomed to failure.

Intelligence

Intelligence provides IW practitioners with assessments of an enemy's ITS and their likely reactions, both human- and machine-directed, following the commencement of an information attack. ITS are dynamic and their configuration can be changed with minimal effort. Planning attacks against such systems requires refinement in response to such changes, often at the last minute and occasionally during an attack. Accordingly, employment of successful MIWT strategies demands comprehensive and real-time intelligence support.

OFFENSIVE RUINOUS IW TOOLS AND TACTICS

The U.S. military has a new mission: Be ready to launch an offensive ruinous cyberattack against potential adversaries, some of whom are stockpiling cyberweapons. Such an attack would likely involve launching massive distributed denial-of-service assaults, unleashing crippling computer viruses or trojans, and jamming the enemy's computer systems through electronic radio-frequency interference.

A few of years ago, an order from the National Command Authority (backed by President Bush and Secretary of Defense Colin Powell) instructed the military to gear up to wage cyberwar. The ability of the United States to conduct such warfare still doesn't exist today.

The military sees three emerging threats: ballistic missiles, cyberwarfare, and space control. The U.S. Space Command, the agency in charge of satellite communications, has begun to craft a computer network attack strategy. This strategy would detail actions to be followed by the Unified Commanders in Chief (CINC) if the president and the secretary of defense order a cyberstrike. The CINCs are senior commanders in the Army, Navy, Air Force, and Marines, deploying U.S. forces around the world.

The IW strategy is detailed in a defense plan called "OPLAN 3600." This plan requires unprecedented cooperation with commercial enterprises and other organizations.

NOTE

Other countries, including Russia, Israel, and China, are further along in building their IW capabilities.

The United States may end up with a new type of weaponry for launching massive distributed denial-of-service attacks and computer viruses. The Chinese are already moving along with this.

In addition to the possibility of cybercombat between nations, the military acknowledges that terrorists without the backing of any country can potentially use cyberweapons to disrupt U.S. telecommunications or banking systems, which are largely electronic. That's one reason the U.S. Space Command is joining with the FBI to build an IW strategy. This requires a close relationship between the military and law enforcement. The FBI will have to help determine if any cyberattack (see sidebar, "Cyberoffense Mired in Cold War") suffered by U.S. military or business entities calls for a military or law enforcement response.

CYBEROFFENSE MIRED IN COLD WAR

The absence of a catastrophic cyberattack against the United States has created a false sense of cybersecurity and has allowed costly Cold War–era Pentagon programs to

→

siphon money from critically needed information technology (IT) and security programs. The United States is still mired in a Cold War–era defense-spending mentality. The rapid advance of IT has created real and potentially catastrophic vulnerabilities. The consequences of a cyberterrorist attack *could be devastating*.

Perception of the Problem

Senior security officials are battling a perception problem according to IW experts. Without a clear-cut example of an electronic Pearl Harbor, where a surprise cyberattack cripples financial markets and other critical systems, it's difficult to convince top military and political leaders that IT research and development should be a bigger priority in the budget process.

Cyberterrorism is not an abstract concept. Although attacks historically have been labeled as "nuisances," that may not be the correct way to look at the problem. The government is dealing with an *enormous educational deficit* when it comes to IT security. Part of the problem is that DoD remains committed to lobbying Congress for money to pay for programs such as the F-22 Joint Strike Fighter instead of increasing funding for IT programs. That is not affordable even in this age of surpluses. DoD's assumptions about future budget gains are wrong. More money should be spent on advanced sensors, precision-guided weapons, and other IT programs. That type of investment would preclude the need to buy costly systems such as the F-22.

Even events such as the outbreak of the "love bug," which reportedly cost the U.S. economy billions of dollars, have not convinced people in and out of government that the problem is real. Usually, when a major crisis costs people a lot of money, it leads to many visits to Capitol Hill and requests for help. That never happened after the love bug outbreak.

Some experts have questioned the government's liberal use of the term *terrorism* to describe acts of mass disruption of the Internet. However, when asked about the seeming lack of interest in cyberattacks by well-known terrorists such as Osama bin Laden, a senior White House official said the focus should not be on what bin Laden does or does not do, but on being proactive and understanding that a major attack may be coming. The United States is attempting to be proactive, but many believe that the United States is going to get seriously nailed.

The National Security Agency (NSA) is one of the federal entities that has taken a proactive approach toward security cooperation between government and industry. However, one of the biggest challenges facing the nation, highlighted during the love bug incident, remains convincing industry that security is as important as making money. Vendors and users have to treat information assurance as a fundamental precept of doing business. It has to become part of the business case.

The Internet is ubiquitous. It allows attacks from anywhere in the world. Attackers can loop in from many different Internet providers. It could start across the street but appear to be coming from China. Something that might look like a hacker attack could be the beginning of cyberwarfare.

NOTE

A cyberattack can include espionage using computer networks.

The growing bullets-and-guns conflict between Israel and the Palestinians, with Islamic supporters elsewhere, is being accompanied by cyberattacks from each side against the other. It's serious enough that the FBI issued an alert about it to the U.S. Space Command, giving U.S. forces warning that the action on the cyber front could affect them as well.

OFFENSIVE CONTAINMENT IW TOOLS AND TACTICS

Of all the activities that have emerged with the evolution of IW and information operations, command and control warfare (C2W) has attracted the most attention. The United States' approach to C2W is comprehensive. This country has committed substantial resources to the development of technologies, doctrine, strategies, and organizations that will equip it to meet an information threat in any future conventional war. Countries like Australia, however, like most non-superpower nations of the world, will not be able to commit the substantial resources needed to follow the American model. Therefore, the general approach discussed in this chapter is tempered by the economic realities that will dictate the degree to which mid-level powers can invest in these strategies.

NOTE

Command and control warfare (C2W) is the approach to military operations that employs all measures (including but not limited to Electronic Warfare [EW], military deception, psychological operations [psyops], operations security, and targeting) in a deliberate and integrated manner, mutually supported by intelligence and ITS, to disrupt or inhibit an adversary's ability to command and control his or her forces while protecting and enhancing our own.

C2W is the war-fighting or tactical application of MIWT and is usually aimed at a specific and defined battlespace, although it may be conducted in conjunction with other MIWT that may be focused on strategic information targets. There are five elements of C2W, covering both offensive and defensive applications:

- Operations security
- Military deception
- Psychological operations

- Electronic warfare
- Targeting

Operations Security

Operations security (OPSEC) is a term that appears in many military documents in almost as many contexts, with several apparently different meanings. OPSEC is a process used for denying adversaries information about friendly disposition, intentions, capabilities, or limitations. It requires the employment of specialist equipment, including software, the adoption of suitable procedures, and most important, the development of a pro-security organizational culture. OPSEC is equally important as a defensive posture as it is in developing offensive strategies. By denying a potential enemy an understanding of the capabilities of friendly systems, possible hostile C2W will be more likely to miscalculate the friendly information capabilities and be ineffective.

Military Deception

Military deception is used to inject ambiguity and create false assessments in the decision-making process of the enemy. The objectives of employing military deception are to create a false deduction of friendly intentions, capabilities, or dispositions by the enemy. The target of deception is the enemy decision maker, that is, the individual who has the necessary authority to make a decision. There is no point to influencing a decision if, in the event of ambiguity, the decision maker passes the decision to a higher authority. In this case, the higher authority must also be the target of deception.

Psychological Operations

Psychological operations (psyops) are operations that are planned activities in peace and war directed to enemy, friendly, and neutral audiences to influence attitudes and behavior affecting the achievement of political and military objectives. The objective of psyops is to cause enemy, friendly, and neutral personnel to act favorably toward friendly organizations. Psyops have been used throughout history to influence adversary leaders and groups. The expansion and development of IT, and associated global media coverage, has enhanced modern psyops opportunities.

Electronic Warfare

Electronic warfare (EW) is the military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum. This action retains friendly use of the electromagnetic spectrum.

Targeting

Targeting is not just a process, nor is it just focused on destructive ends. Targeting is a capability that emphasizes the requirement to collect, process, and interpret information regarding decisive points in an enemy's C2 system and then selects the most effective option of incapacitating them. There are many hard- and soft-kill options available to a commander. Soft-kill options include the use of EW, strategic computer operations, and information weapons, whereas hard-kill options refer to the various means of physically destroying targets.

Hard or soft destruction requires the capability to remove selected targets from an enemy's order of battle. These targets include vital communication nodes, national infrastructure, vital personnel, and specific military equipment. Destruction may be achieved by any arm of the military. Physical destruction carries the highest risk and, unlike the other elements of C2W, tends to be permanent; that is, buildings are destroyed and people are killed. This can be either a desirable or undesirable outcome, and so must be considered when strategies are being developed. The diplomatic recovery time for physical destruction is usually considerably longer than that of the other elements. Accordingly, even though it is often the most effective method of demonstrating resolve, physical destruction is generally used as a last resort. However, a commander must have the option of employing hard- and soft-kill options to accomplish a desired C2W effect.

The Objective of C2W

Until the 1991 Gulf War, the C2W elements had rarely been used in conjunction with each other to specifically target an enemy's ability to command and control its forces. In the Gulf War post-mortem, the advantages of combining the five elements in pursuit of a single objective were realized and true C2W was born.

The ultimate objective of C2W is to decapitate the enemy's command structure from its body of combat forces while ensuring the integrity of friendly C2 systems. C2W aims to reduce the uncertainty of combat by creating a battlespace that becomes more predictable for friendly forces as the C2W effort increases, while becoming exponentially less predictable for the enemy. C2W activities are designed to lift the fog of war for friendly forces while thickening the fog for the enemy. C2W strategies focus the five elements specifically on the decision cycles of both friendly and enemy forces. Therefore, the aim of C2W is to gain, maintain, or widen a gap in the effectiveness of C2 in favor of friendly forces throughout a campaign and particularly at decisive points in a battle.

C2W and the OODA Loop

The often-quoted observation, orientation, decision, action (OODA) loop has been adopted as the focal point of C2W. The concept of the OODA loop has its origins in the Korean War, where an American pilot identified the advantages of having good visibility and sensitive controls on board the U.S. Sabre jet fighters. Although the Russian MIG 15s were faster, more powerful, more maneuverable, and could sustain greater bank angles, the American jets were consistently victorious in air-to-air engagements. The U.S. pilots simply had a shorter total period between observing an event, orientating themselves to the possible ramifications of the event, making a decision, and acting. The value of a relatively short decision cycle was realized. Since the inception of air-to-air combat, staying inside the enemy's decision loop has been a consistent objective. This has been a recognized objective of many forms of warfare.

The OODA loop concept is now applied to most aspects of modern warfare, from land maneuvers to strategic missile developments. The OODA loop can also be seen to operate in the business world. Those who are quick to observe an opportunity, recognize the opportunity, and exploit the opportunity are more frequently the successful or victorious business persons. The OODA loop theories can be found in the heart of modern C2 systems and, consequently, in modern C2W strategies. Successful C2W operations will, therefore, increase the enemy's decision cycle (his or her OODA loop) to such a point that he or she will become increasingly vulnerable to attack.

C2W in the Gulf War

In the 1991 Gulf War, the Coalition forces attacked the Iraqi C2 system from the outset. Even before the war had commenced, EW, psyops, and deception were employed to influence the Iraqi people and hierarchy. During the first hours of the air attacks in Iraq, ITS and communication devices were targeted, and in many cases physically destroyed, leaving the huge force that had occupied Kuwait completely cut off from the commanders in Baghdad. The Iraqi air defense system was virtually shut down by coalition activity within hours of the commencement of Operation Desert Storm. The extant Iraqi air defense system was among the most extensive in the world. Shutting such an extensive system down with apparent ease was a significant achievement and the result of a calculated offensive involving all of the C2W elements. This early success gave the coalition forces air supremacy. In turn, this supremacy significantly reduced the potential for coalition air fatalities and allowed the coalition air forces to strike Iraqi ground targets almost at will. The coalition forces effectively destroyed the ability of the Iraqi military commanders to observe, and the Iraqi OODA loop was significantly lengthened.

In the 2003 Operation Iraqi Freedom, defense of friendly C2 systems and attacks on enemy systems were of paramount importance. The United States had the shortest decision cycle and thus had a decisive advantage. A confused army leads to another's victory.

DEFENSIVE PREVENTIVE IW TOOLS AND TACTICS

Eight years after the military pioneered intrusion detection systems, the DoD now requires its massive networked systems to be protected by round-the-clock intrusion detection monitoring to defend against hacker and denial-of-service attacks. The DoD has developed a policy that mandates the use of intrusion detection systems in all military networks. The DoD has more than 69,000 computer networks that handle everything from weapons systems C2 to inventory to payroll. Roughly 15% of DoD networks, such as satellite links, are considered mission-critical.

Under this draft policy, every DoD entity needs to have a computer network-detection service provider, which could be a DoD entity or a commercial entity. Thus, the Defense Information Systems Agency (DISA) is responsible for defining the intrusion detection plan. Whether the Navy, Army, or Air Force should buy commercial intrusion detection software or entrust network protection to an outside service provider should be decided on a case-by-case basis.

The military helped pioneer intrusion detection systems by building its own software from scratch in 1996. Since then, various parts of the military have deployed products from vendors that include Internet Security Systems, Symantec, Cisco [3], and Network Ice. Today, still only a small percentage of the military's overall networked systems are guarded by any form of intrusion detection. When the final decision on the mandatory intrusion detection systems will arrive is still unclear, but deliberations taking place among the military's Joint Chiefs of Staff underscore their determination to do whatever it takes to prevent hackers and denial-of-service attacks from disrupting its networks.

Some defense-related agencies, such as the secretive NSA in Fort Meade, Maryland, already require round-the-clock monitoring of computer hosts and networks. Every system within the NSA is monitored. In the Defense Intelligence Agency, it's the same sort of situation.

One difficulty in deploying intrusion detection software is that it must be regularly updated to include new attack signatures, because new hacker exploits are discovered all the time. In addition, intrusion detection software can record "false positives," a false alarm about trouble, and software occasionally needs to be fine-tuned to work correctly. These types of challenges, along with the difficulty in hiring security experts to manage intrusion detection, is spurring security services in which intrusion detection is done remotely in the service provider's data centers or with hired help onsite.

Not all attempts by the federal government to put large-scale intrusion detection systems in place have succeeded. In 2000, President Clinton unveiled his goal of creating the Federal Intrusion Detection Network as part of what was called the National Plan for Information Systems Protection. FIDNet, as it was called, was envisioned by the White House as a government-wide intrusion detection network to monitor activities across civilian and defense networks. The idea, though, generated a firestorm of criticism from civil liberties groups that argued that FIDNet's monitoring of citizens would constitute an invasion of privacy [4]. Although the General Services Administration (GSA) issued a draft RFP for FIDNet, GSA indicates the idea has been shelved.

Others are just not sold on the idea of outsourcing security to services providers. They've opted not to go with managed security. With managed security services, you give away the keys to the castle in some respects. Therefore, any organization that wants to take advantage of managed security services has to share detailed knowledge about its operations so that intrusion detection systems can be properly used.

DEFENSIVE RUINOUS IW TOOLS AND TACTICS

In 2002, the Pentagon formed five technology centers, which are staffed by reservists who work in the private sector by day and spend one weekend per month defending the DoD against cyberattacks through the use of defensive ruinous IW tools and tactics. The deputy secretary of defense approved a plan that would establish five joint reserve virtual information operations (JRVIO) and information assurance organizations. The centers' mission is to ensure that American war fighters dominate the computer information domain in future conflicts, according to the Pentagon.

Information operations has emerged as an area that is extremely well suited to the integration of reserve capabilities. Members of the reserves and National Guard are often way ahead because of the very nature of their civilian employment, trained in their workplaces to exploit technology.

The DoD has long been battling a high-tech brain drain spurred by a booming economy and the lure of higher-paying jobs in the private sector. The change has made the National Guard and reserves a repository of high-tech skills. At the same time, the Pentagon is facing an increase in cyberattacks and intrusions and has increased its focus on using cybertactics to fight future conflicts. The teams could be involved in a wide range of efforts, including enemy computer network attacks, defense of U.S. critical infrastructures, psychological operations, intelligence support, vulnerability assessments, and reviews of Pentagon Web sites for sensitive information.

The Pentagon expects 526 reserve officers and enlisted personnel to staff the five JRVIOs during fiscal 2005 and 2006 in Maryland, Virginia, and Texas. However, from 2007 to 2011, that number is expected to expand to more than 1,000. The initiative is a result of a two-year Pentagon study called "Reserve Component Employment 2006." That study recommended the formation of a cyberdefense unit that would consist of people with IT skills who could work in different locations instead of at a single center. The study also urged the department to recruit high-tech-savvy people from the private sector.

DEFENSIVE RESPONSIVE CONTAINMENT IW TOOLS AND TACTICS

One of the more recent additions to the military commander's toolbox are defensive responsive containment IW tools. Computers and associated technology have helped change the face of modern information warfare tactics by providing the capabilities to generate and process massive amounts of data and disseminate the resultant information throughout the battlespace. However, computers provide more than just an information-processing capability. They may also be used as weapons in their own right. The most common examples of computer operations include hacking, virus planting, and chipping. These techniques are primarily aimed at targeting the enemy's broad information environment. However, they may also be used to attack the enemy's computer-based weapon systems and computer-based platforms, such as "fly-by-wire" aircraft. Although generally strategic in nature, computer operations may be applied to the tactical and operational components of the conventional warfare environment, either in support of C2W operations or in direct support of air, land, or sea operations.

Hacking

The term *computer hacker* is now synonymous with *computer criminal*, although, arguably, this merging of terms is not justified. Someone who uses a computer to rob a bank is a criminal, not a hacker. The genuine computer hackers are still doing what the original computer hackers were doing 43 years ago—exploring the bounds of computer science.

Unfortunately, exploring today's computer science often means entering other people's systems. There are many computer hackers around the world who enter other people's systems on a daily basis. Most simply gain access to the systems, snoop around for a while, and leave. Some hackers like to explore the logic flow in systems. A few like to exploit these systems for either their own gain or simply to make life difficult for the users of that system. The genuine hackers, while invading system privacy, rarely damage the systems into which they have hacked. However, most users of systems understandably find it an unacceptable invasion of their privacy to have people intruding into their systems.

Hackers present a genuine problem to most organizations today and a specific threat to military security. Hackers have historically found the challenge of breaking into so-called secure military systems one of the more satisfying aspects of their hobby. Accordingly, the first and foremost aim of any information strategy for military forces must be to defend their own system integrity.

Once access is gained into a system, hackers can generally manipulate whatever files they wish. They will often set up personal accounts for themselves in case they wish to return again in the future. A hacker can, of course, collect very important information. In the business domain, intelligence can be gained about a competitor's product. In the government service domain, sensitive personal information can be obtained (or altered), which can later be used against individuals. In the military domain, classified information such as capabilities, vulnerabilities, strategies, and dispositions may be extracted or manipulated. A hacker can also change the file structure, amend the logic flow, and even destroy parts of the system.

Hacking is no longer simply a pursuit of misfits and computer scientists; it is now a genuine method of obtaining information by government agencies, criminals, and subversive organizations. There have been several reports about government sponsorship of such activity. Many of the world's secret security organizations are now passing industrial secrets to their nation's domestic businesses. The basic tool kit of today's industrial spy consists of a PC and a modem. The industrial spy is simply a hacker who intrudes into someone else's computer system and then exploits the information obtained. Neither domestic nor international laws adequately address all of the issues surrounding hacking. Therefore, in the unlikely event that hackers are caught, in many situations prosecution is impossible.

The impact on those involved in developing MIWT is that hacking presents a genuine threat to the security and integrity of both military and civilian information systems. Defense against hacking can be successful to varying degrees. Most defensive strategies are system dependent; therefore, listing them in this chapter would be pointless. However, defense against hacking needs to be considered by anyone who manages or operates an IT system.

The other reason national security forces should become involved in hacking is the potential benefits that can be derived by employing hacking techniques as an offensive tactic. Intelligence collection of information stored in an enemy's databases as well as the specific system capabilities, vulnerabilities, and architecture can be accomplished successfully using hacking techniques. In future wars, information derived from hacking will form a large part of intelligence databases and, thus, manipulation of the enemy's decision-making support systems will become routine.

Viruses

A virus is a code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces. Protecting against computer viruses has become a part of using modern ITS. Viruses are passed from computer to computer via disks and reportedly via the more recent practice of electronic file transfer, such as email. Although statistics concerning viruses are often difficult to substantiate, some specialists estimate that there are as many as 11,233 viruses currently existing on the Internet, with cures being available for only 4,583. Although virus screening software should prevent known viruses being brought into a system, they will not prevent all virus attacks. The most effective method of minimizing the risk of virus attack and minimizing the damage caused by viruses in the event of an attack, is by employing sound and rigorous information-management procedures.

Isolating Internet systems from operating systems where practical is vital, and minimizing computer-to-disk-to-computer transfers, particularly if the origin of that data is the Internet, will reduce the chances of picking up a virus. The use of the most recent anti-virus software and the screening of disks every time they are placed in a computer will reduce the risk of disk infections being passed onto systems. Careful selection and management of passwords may deter a potential intruder from accessing a system and planting a virus, while the maintenance of comprehensive system backups can minimize the impact of viruses, should one find its way onto a system. Viruses, however, can also be backed up, and a dormant virus can infest any backup files and can be reintroduced when a system is recovered. Accordingly, a layered backup strategy is imperative. Anti-virus strategies are aimed at minimizing the chances of getting a virus and minimizing the damage that viruses can cause if they are introduced. Users of today's ITS must be aware of the virus threat. Simple procedures will often be enough to avoid viruses, but a single failure to comply with anti-virus procedures can result in systems becoming inoperable.

Virus planting is clearly a suitable and attractive weapon for military forces and is a valuable addition to the offensive information operations inventory. If a simple virus can be injected into the systems of a potential enemy, the need to expend effort in physically attacking that system may be eliminated.

Chipping

Most people are aware of the vulnerability of software to hostile invasions such as a virus attack. Few, however, are aware of the risk to the essential hardware components of an ITS. *Chipping* refers to unexpected events that can be engineered into computer chips. Today's chips contain billions of integrated circuits that can easily be configured by the manufacturer to initiate unexpected events at a specific time or at the occurrence of specific circumstances. This may explain why some electronic goods fail a short time after the warranty has expired. There is almost no way of detecting whether a chip contained within a piece of equipment has been corrupted.

One way to minimize the risk of chipping is to self-manufacture all important chips, such as those used as part of an aircraft's flight control system. Economically, this is often not feasible. Most chips used within today's high-technology equipment are manufactured in countries where labor costs are low. Establishing an indigenous manufacturing capability would increase the cost of acquiring the equipment. A risk assessment must be made when purchasing vital equipment from overseas, by comparing the risk of vital equipment failing once hostilities commence to the cost of producing chips internally or developing rigorous quality control of imported chips.

Chipping represents a simple way to develop a conventional military advantage by those countries that regularly export military equipment. In the event of any hostilities with recipients of their chipped equipment, that equipment could be incapacitated without having to use conventional force. This makes economic as well as military sense. The legal and ethical aspects are a separate issue.

Many other computer weapons can be used in conjunction with or instead of chipping, viruses, and hacking. These weapons have many different descriptive names such as worms, trojan horses, and logic bombs and are commonplace in today's information society. They are all examples of computer operations that may be adapted to suit the IW environment. A detailed description of all of these techniques is beyond the scope of this chapter. Suffice to say that computer weapons should be an integral part of any IW operations strategy. They should be considered valid alternatives to conventional weapons both in offense and defense.

COUNTERING SUSTAINED TERRORIST IW TACTICS

Terrorism is, among other things, a weapon used by the weak against the strong. The United States has moved into the 21st century as a preeminent, global power in a period of tremendous flux within societies, among nations, and across states and regions. Terrorism will accompany changes at each of these levels, as it has in other periods of flux in the international environment. To the extent that the United States continues to be engaged as a global power, terrorism will have the potential to affect American interests directly and indirectly, from attacks on U.S. territory (including low-probability but high-consequence "superterrorism" with weapons of mass destruction) to attacks affecting the United States' diplomatic and economic ties abroad or the United States' ability to maintain a forward military presence or project power in times of crisis. The United States will also have a unique, systemic interest in terrorism as a global problem (including acts of domestic terrorism confined within state borders, which make up the bulk of terrorism worldwide) even where the United States is not directly or even indirectly targeted. In one way or another, terrorism can affect the United States' freedom of action, not just with regard to national security strategy narrowly defined, but across a range of compelling issues, from drugs and money laundering to information and energy policy.

Many of the United States' high-priority national objectives have been shaken by the recent experience of terrorism. The Oklahoma bombing and the 9-11 World Trade Center and Pentagon terrorist attacks struck at the United States' sense of security within its borders. Attacks against U.S. forces in Saudi Arabia raise questions about the United States' strategy for presence and stability in an area of critical importance for world energy supply. The bombings of the U.S. embassies in Kenya and Tanzania and of the *U.S.S. Cole* in Yemen raise questions about the exposure that comes with active engagement in world affairs and point to the risks of privately sponsored terrorism. The assassination of Prime Minister Rabin, the increased campaign of suicide bombings in Israel, the death of Yasser Arafat, and the refusal of the Bush administration to deal seriously with the Palestinians continues to put the Middle East peace process in serious jeopardy, threatening a critical and long-standing U.S. diplomatic objective. Elsewhere, terrorism has destabilized allies (in Saudi Arabia, Egypt, and Turkey) and has rendered counternarcotics relationships difficult (in Colombia and Mexico). Where societies and regions are fundamentally unstable, and where political outcomes are delicately poised, terrorism will have a particular ability to affect strategic futures.

Overall Observations

Most contemporary analyses of terrorism focus on terrorist political violence as a stand-alone phenomenon, without reference to its geopolitical and strategic context. Similarly, counterterrorism policy is rarely discussed in terms of its place in broader national security planning. Prior to the specter of superterrorism, using weapons of mass destruction, terrorism, however horrible, never posed a threat to U.S. security. With the important exception of weapons of mass destruction, terrorism still does not pose a grave threat to America's future as it does to many other societies around the world. However, many types of terrorism do pose a threat to U.S. interests, from homeland defense to regional security and the stability of the international system. As a global power, the U.S. perspective on terrorism is bound to differ in substantial ways from that of others, including allies such as Britain, France, and Israel, whose experiences provide lessons, but not necessarily direction for U.S. counterterrorism policy. In light of the preceding IW arsenal and tactics analysis of the military, certain overall sustained terrorist IW tactics observations stand out:

- Terrorism
- Geopolitics of terrorism
- Counterterrorism versus new terrorism

- U.S. Exposure
- Comprehensive counterterrorism strategy

Terrorism

Terrorism is becoming a more diverse and lethal problem. Contemporary terrorism occupies an expanded place on the conflict spectrum, from connections to drug trafficking and crime to its use as an "asymmetric strategy" by state and non-state adversaries in a war paradigm. For a variety of reasons, primarily the rise of religious cults with transcendent agendas, but also the hardening of established political groups, terrorism has become more lethal. With the potential for catastrophic terrorism using weapons of mass destruction, lethality could increase dramatically.

Geopolitics of Terrorism

The geopolitics of terrorism are changing. Over the next decades, the prevailing image of terrorism affecting U.S. interests as a problem emanating largely from the Middle East is likely to be overtaken by a more diverse set of risks. The Balkans, the former Soviet Union, and Latin America are set to emerge as significant sources of terrorism aimed at or affecting U.S. civilian and military activities. Moreover, the vast bulk of global terrorism will continue to be confined within the borders of affected states. More anarchic futures in the third world could fuel this type of terrorism, threatening America's systemic interests as a global power and placing constraints on the United States' international engagement.

Counterterrorism Versus New Terrorism

Much counterterrorism experience is losing its relevance in light of the "new" terrorism. Many established images of counterterrorism policy, especially the use of force against state sponsors, are losing their relevance as traditional forms of terrorist behavior and organization (largely a product of the ideological and national liberation movements of the 1960s–1980s) give way to new patterns. The new terrorism often lacks a detailed political agenda against which the use of violence can be calibrated. It is therefore more lethal. It is less hierarchical in organization, more highly networked, more diffuse in membership and sponsorship, and may aim at disruption as well as destruction. The absence of clear-cut sponsorship, above all, will complicate the task of deterrence and response. It will also compel a reorientation of policy to target nonstate sponsors and individual suspects.

U.S. Exposure

Foreign experts see U.S. exposure increasing but view the problem in narrower terms. A survey of expert British, French, and Israeli perspectives yields a gloomy outlook with regard to U.S. exposure to terrorist risks, which are widely seen as increasing, particularly with regard to U.S. forces in the Persian Gulf. Policy makers and observers in these allied countries are not surprisingly focused on specific national risks, few of which are analogous to risks facing the United States at home and abroad. With the limited exception of France, which has a global and expeditionary outlook in strategic terms, terrorist challenges are generally viewed in narrower, but starker, terms. Notably, experts in all three countries share a degree of skepticism about technology as a solution in counterterrorism.

Comprehensive Counterterrorism Strategy

A comprehensive counterterrorism strategy should have core, environment shaping, and hedging components. Treating terrorism as one of many national security challenges suggests a multidimensional approach. Core, longer-term strategy must a ddress the political, economic, and social roots of international terrorism; make deterrence relevant to non-state actors as well as state sponsors; and reduce the risk of truly catastrophic terrorism using weapons of mass destruction. The environment-shaping aspect aims to create conditions for successfully managing terrorist risks, making terrorism more transparent, shrinking "zones of chaos," harnessing key alliances to the counterterrorism effort, reducing U.S. exposure, and cutting off terrorism's resources. Finally, the United States can hedge against inevitable terrorism by hardening policies as well as targets and preparing to mitigate the effects of increasingly lethal terrorist acts.

Implications for Military Strategy and the U.S. Air Force

In many instances, air and space power will not be the best instruments in the U.S. counterterrorism arsenal, and air power will rarely be used independently against terrorism. However, air and space power can play a role in intelligence and covert action. There will also be instances, as in the past, where air and space power will be instruments of choice in the fight against terrorism. Moreover, terrorism and counterterrorism policy are changing in ways that will significantly affect the future contribution of air- and space-based instruments.

Events in Sigonella (Sicily) and Afghanistan as well as Operation El Dorado Canyon may be key models for the future. Air power in the service of counterterrorism will include, but will also go beyond, the surveillance and punishment of state sponsors. Deterrence and response will likely evolve in the direction of a more "personalized" approach, emphasizing the monitoring and attack of key nodes in terrorist networks and the forcible apprehension of terrorist suspects—with or without the cooperation of local states. Future demands on air power may be driven as much by requirements for intercepting and extracting suspects as by the need to attack terrorist training camps and strike regimes supporting the export of terrorism.

Air and space power will help make terrorism (an inherently amorphous phenomenon) more transparent. The ability to identify and to target terrorist-related activity and to help expose terrorism and its sponsors to policy makers and international opinion will be key contributions of air- and space-based assets. As terrorism becomes more diffuse and its sponsorship increasingly hazy, finding the "smoking gun" will become more difficult but essential to determine strategies and build a consensus for action. Space-based sensors, surveillance by Unmanned Aerial Vehicles (UAVs), and signals intelligence (SIGINT) will facilitate the application of air power and other instruments in the service of counterterrorism.

Gaining leverage in addressing the new terrorism will be a key strategic and technical challenge. Future requirements for counterterrorism will be part of a broader need to tailor air and space power to challenges posed by non-state actors, including networks of individuals. At the same time, policy instruments, including air and space power, will need to concentrate on detecting and preventing the use of weapons of mass destruction by terrorists—whether as a stand-alone apocalyptic act or as a low-tech delivery system in the hands of adversaries.

Much terrorism (and counterterrorism action) will focus on urban areas, with strong political and operational constraints. Terrorism is increasingly an urban phenomenon worldwide. One explanation for this is that the political fate of most modern societies is determined by what happens in cities. Terrorists seeking to influence political conditions have many incentives to attack urban targets. Terrorists with transcendental objectives will, similarly, find symbolic and vulnerable targets in urban settings. The use of air power in a counterterrorist mode introduces the more general problem of operating in an urban environment (the difficult Israeli experience in Beirut and South Lebanon is instructive). Terrorists and their facilities will be difficult to locate and target. Operations against them or to rescue hostages will pose severe challenges for the use of air power, not least the risk of placing uninvolved civilians in harm's way. The viability of air power as an instrument in such settings may depend on the capacity for discriminate targeting and the use of less-than-lethal technologies.

Air power's pervasiveness and speed are advantages in the face of transnational and transregional terrorism. In an era in which terrorist acts may take place across the globe and where sponsors cross national and regional lines, counterterrorism strategies will become "horizontal" in character. Where terrorists and their sponsors can be identified and attacked with purpose, the global sight and reach of air- and space-based assets will be valuable to national decision makers.

Air and space power will have a synergistic effect on other counterterrorism instruments. Air and space power can be used in concert with covert action, diplomacy, economic instruments, and joint military operations. The notion of "parallel warfare," developed in relation to attacks on infrastructure in war, will also be relevant to counterterrorism operations. Operations using a range of instruments can be designed to act, in parallel, on terrorist supporters, terrorist infrastructure and networks, and the terrorists themselves.

DEALING WITH RANDOM TERRORIST IW

During the 1970s and 1980s, political extremism and terrorism frequently focused on "national liberation" and economic issues. The collapse of the Soviet bloc and the end of its covert funding and encouragement of terrorism led to a decline in the militant and violent left-wing terrorist groups that were a feature of the age.

The 1990s through the present have seen the development of a new terrorism: random terrorist IW. This is not to say that state-backed terrorism has ceased, but rather that the spectrum of terrorism has widened. This new extremism is frequently driven by religious fervor, is transnational, sanctions extreme violence, and may often be millenialist. The new terrorism may seek out military or government targets, but it also seeks out symbolic civilian targets, and the victims have mostly been innocent civilians (Alfred P. Murrah Building, Oklahoma City; World Trade Center, New York; AMIA Headquarters, Buenos Aires; etc.).

Growing concern about this new terrorism has been paralleled by concern about the employment of the new information and communication technologies (ICTs). ICTs offer a new dimension for political extremists and terrorists. They allow the diffusion of C2, they allow boundless new opportunities for communication, and they allow the players to target the information stores, processes, and communications of their opponents. The sophistication of the modern nation-state, and its dependency on computer-based ICTs make the state ever more vulnerable.

The use of ICTs to influence, modify, disrupt, or damage a nation-state, its institutions, or population by influencing the media or by subversion has been called "netwar." The full range of weapons in the cyberspace armory can be employed in netwar—from propaganda campaigns at one level to interference with databases and networks at the other. What particularly distinguishes netwar from other forms of war is that it targets information and communications and may be used to alter thinking or disrupt planned actions. In this sense, it can be distinguished from earlier forms of warfare—economic wars that target the means of production and political wars that target leadership and government.

Netwar is therefore of particular interest to those engaged in nonmilitary war and those operating at the sub-state level. Clearly, nation-states might also consider it as an adjunct to military war or as an option prior to moving on to military war. So far, however, it appears to be of greater interest to extremist advocacy groups and terrorists. Because there are no physical limits or boundaries, netwar has been adopted by groups who operate across great distances or transnationally. The growth of such groups, and their growing powers in relation to those of nation-states, suggests an evolving power-based relationship for both. War in the future is more likely to be waged between such groups and states rather than between states.

Most modern adversaries of nation-states, in the realm of low-intensity conflict—such as international terrorists, single-issue extremists, and ethnic and religious extremists—are organized in networks, although their leadership may sometimes be hierarchical. Law enforcement and security agencies therefore often have difficulty in engaging in low-intensity conflict against such networks because they are ill-suited to do so. Their doctrine, training, and modus operandi have, all too often, been predicated on combating a hierarchy of command like their own.

Only now are low-intensity conflict and terrorism recognized as strategic threats to nation-states, and countries that, until very recently, thought terrorism was something that happened elsewhere have become victims themselves. The Tokyo subway attack by the Aum Shinriko, the Oklahoma City bombing and the 9-11 terrorist attacks, would have been unthinkable a generation ago. Not only was the civil population unprepared, but so was the law enforcement population, despite clear warning signs that such attacks were in the offing.

Cyberspace is becoming a new arena for political extremists: the potential for physical conflict to be replaced by attacks on information infrastructures has caused states to rethink their concepts of warfare, threats, and national assets at a time when information is recognized as a national asset. The adoption of new information technologies and the use of new communication media, such as the Internet, create vulnerabilities that can be exploited by individuals, organizations, and states.

Also, the arrival of the Internet has provided the first forum in history for all the disaffected to gather in one place to exchange views and reinforce prejudices. It is hardly surprising, for example, that the right-wing militias' favorite method of communication is email and that forums on the Internet are the source of many wild conspiracy theories that drive the media.

Preeminent among the extremists and terrorist groupings who have entered cyberspace faster and more enthusiastically than others, are the far right, that is white supremacists and neo-Nazis and radical Islamists. Others, such as eco-extremists and the far left appear to be slower in seizing the opportunities available.

What characterizes these two groups are their transnational natures. The far right is increasingly active in the United States and Europe, but, in contrast to its ideological roots in the 1920s and 1930s, it seeks now to unite a white Anglo-Saxon, or Europe-originating, entity in a rear-guard action to oppose centralized democratic government and return to some imagined past world in which an armed, racially pure, white man can live untroubled by the police, the Internal Revenue Service, and the world banking system. The Islamist diaspora, now spread worldwide, seeks a return to divine-ruled states (or even one transnational state) in which all Muslims will live under the norms and laws of the Saudi Arabian peninsula in the first and second centuries of the Common Era. These types of organizations make them ideal users of networks and proponents of netwar. Their ideas and their use of cyberspace will be further discussed in Chapter 15.

Although the use of ICTs to enhance C2 and enhance communication is apparent among Islamist extremists and among the militia movement and far right in America, it is less so among far right and other extremists in other parts of the world. This clearly reflects the more widespread ICT access in North America. Fears by Western governments that their national infrastructures may be a target for IW or cyberterrorism may be well founded, but the evidence so far is that sub-state groups at least use ICTs mainly for propaganda, secure communications, intelligence gathering, and funds management.

One observer noted that the Internet has not replaced other communication media for the far right and that its largest use in this regard has been to advertise the sale of non-Internet-related propaganda, such as books, audiotapes, and videos. Nor has the Internet led to an increase in mobilization. The Seattle-based Coalition For Human Dignity observed that far right events in the United States, which were heavily promoted on the Internet only, were failures.

For some on the American far right, the Internet has become an end in itself. Surfing the Net has replaced real action. It is a measure of how degenerate and weak the U.S. movement has become that some people actually think this is a good thing. Not only do individuals want risk-free revolution, they now want people-free revolution. Here lies the great danger of the computer for everyone who uses it. It allows individuals to spend their lives interacting with a machine rather than with people.

However, it does not pay to be complacent; extremists and terrorists are increasingly IT literate. Unless law enforcement and national security agencies can move quickly, they will leave national infrastructures defenseless. For example, these terror networks understand the Internet and know that law enforcement agencies lag far behind in both skills and available technologies.

Therefore, what is significant for the far right and its use of the Internet is that it possesses the potential to offer the relatively small numbers of people involved a means to communicate, develop a sense of common purpose, and create a virtual home symbolically. The Internet combines both intimacy and remoteness. These properties make it uniquely suitable for maintaining relationships among groups that are prone to attrition, because forms of association can be established at a social and geographical distance.

Although some futurists warn of an electronic Pearl Harbor, the reality is that terrorists have not yet resorted to strategic IW. What is apparent, however, is that warfare is shifting toward attacking civilian targets and that sub-state terrorists and other extremists are increasingly targeting civilian infrastructures. Increasingly, the perpetrators and the victims of netwar will be from the civilian sphere. It is therefore the civilian infrastructure that is the most vulnerable; the military can protect its own infrastructure, despite media reports that it is vulnerable and a constant victim of hacking.

Governments are becoming increasingly concerned about protecting their own national infrastructures, but global connectivity has grown to such an extent that it is now possible to talk only of a global informational infrastructure. There is only a global information infrastructure. There is no way to draw a line around the continental United States and say that the information infrastructure belongs to the United States. This is true because there is no way to sever the United States from the information infrastructure that connects the rest of the world. What that means is that the U.S. infrastructure is accessible not only to their friends around the world but also to their potential foes. It is just as easy now to engage in a cyberattack from Tehran as it is from Pomeroy, Ohio.

Countering Sustained Rogue IW

Countering sustained rogue IW is envisioned as a new dimension of IW, bringing rogue conflict into the Information Age. Rogue IW offers combatants the ability to execute asymmetrical attacks that have nonlinear effects against an adversary. By targeting or exploiting information and information processes, an attacker can use limited resources to reap disproportionate gains. Furthermore, rogue IW offers weaker enemies (even at the sub-state level) a strategic alternative to attrition—an attractive feature, especially when facing an opponent with significantly stronger conventional forces. Such potential adversaries could perpetrate a rogue IW attack against the United States, using relatively limited resources, exploiting the U.S. reliance on information systems. Targets of such attacks might include C2 networks, satellite systems [5], and even the power grids of the continental United States. Such an attack could potentially have a strategic impact on the national security of the United States.

In contrast, terrorism has been used by states and sub-state groups for millennia. As an instrument to pursue political or social objectives where the user lacks the strength or the political wherewithal to use conventional military means, terrorism has been especially attractive. The intended target of a terrorist act goes beyond the immediate victims. Terrorists create a climate of fear by exploiting the information dissemination channels of its target population, reaching many by physically affecting only a few. The United States experienced a tragic example of this effect in the 1983 bombing of the U.S. Marine barracks in Beirut, the *USS Cole* in Yemen in 2000, and the 9-11-2001 terrorist attacks, where a small terrorist group, clearly weaker than the U.S. military, nevertheless executed an effective strategic attack against the United States.

The problem of rogue IW is not lack of capabilities, but of management and organization. The capabilities are out there already; they just are not being tapped. This problem has only recently emerged as a potentially new warfare area for most defense planners. The problem of terrorism, on the other hand, has been in the headlines and in the social consciousness for decades, especially since the technological advance of intercontinental flight. This section briefly examines these two phenomena conceptually, operationally, and organizationally, seeking commonalities. If comparisons are substantiated as more than circumstantial, then the lessons that might be applied to rogue IW defense from successes and failures of 33 years of countering terrorism should be examined closely. Within the context of these comparisons, this section will also attempt to ascertain whether there is an emergent structure or organization that suggests a correct approach to countering sustained rogue IW.

The bombing of the Murrah Building in Oklahoma City and the 9-11 terrorist attacks were two of many major events to remind the military that the continental United States no longer offers sanctuary from terrorism. Geographical borders probably will never offer sanctuary from rogue IW attacks. The military should organize and prepare for potential rogue IW attacks against them without necessarily having a formal definition and without having to experience a massive information attack. Establishing a rogue IW focal point involves a partial framing of the problem, at least identifying key contributors to its solution. A wide-scale information attack could involve systems under the responsibility of agencies across the government and even the commercial sector. A solution will draw on contributions from areas broader than simply military and law enforcement. In the case of the Oklahoma City bombing, organizations such as Bureau of Alcohol, Tobacco, and Firearms (ATF) and the FBI investigated the incident, and the Federal Emergency Management Agency (FEMA) responded with crisis mitigation using both federal and local resources. In a "digital Oklahoma City," who would take FEMA's place for crisis mitigation? Will local support be available? At present, no framework coordinates a response to rogue IW attacks, and establishing an ex post facto framework in response to an attack is unwise.

Clearly, rogue IW defense will demand many resources throughout the federal government. This does not, however, justify creation of an all-encompassing body tasked with jurisdiction and execution over all aspects of rogue IW. For example, terrorism policies under President Reagan suggested that such an organized U.S. counterterrorism agency (whether newly created or placed within an existing agency) would not have been feasible. This solution fails to take into account the nature of terrorism and the influence of bureaucratic politics. Terrorism is a complex phenomenon requiring a comprehensive response. No agency within the U.S. government possesses the vast array of capabilities needed to combat terrorism effectively. It would be difficult, if not impossible, to create a single department with the needed jurisdiction to control the U.S. response to terrorism and would lead to even greater policy and process problems.

These problems are also inherent in organizing for rogue IW defense (IW-D). Furthermore, the distributed nature of the problem implies a distributed response from the agencies owning the appropriate capabilities. This distributed response, however, should be overseen by a higher office so that the left hand knows what the right hand is doing and so these complex activities are coordinated. An IW-D Oversight Office should be endowed with an independent budget and tasking authority to coordinate the decision-making process, identify capabilities needed to respond, and inform the agencies that own the capabilities as to their defensive rogue IW roles. Staffing this office would be "point members" of the represented agencies, who would then coordinate requirements within their respective agencies. This type of organization resembles, at a much broader range, the joint staff of the DoD, but with a budget as well as tasking authority for IW-D. Furthermore, the office could solicit and coordinate intelligence requirements from the various members of the intelligence community.

DoD has also articulated a similar concept for an office within the Executive Office of the President, organized for countering terrorism, as a potential focal point for the oversight of the U.S. antiterrorist program. This office would be a permanent body with a White House perspective; such a staff could monitor and coordinate activities of the line agency and departments, identify needed capabilities, identify special resources that might be mobilized if an international incident occurs, pull together current intelligence and ongoing analysis and research efforts, identify terrorist incidents, develop scenarios, and formulate plans. It would see that the necessary resources and capabilities are there when they are needed. In an actual crisis, it could function as a small battle staff for decision makers.

An Executive IW-D Oversight Office would be in a prime position to identify and coordinate the investigative agencies, defense organizations, and all elements of the intelligence community that would be in positions to recognize and respond to attack. An IW-D Oversight Office might be led by a director with cabinet rank and a seat on the National Security Council (NSC). Such an office should also interact with the commercial sector, reflecting the extent to which commercial interests would be affected in IW and the contribution industry can make to solutions. Such interaction with the private sector might not be possible with existing agencies because of the baggage that extant agencies might bring to the table.

In addition to reorganizing the bureaucracy, an IW-D Oversight Office might reorganize priorities. Response strategies should not focus on protection as the only priority. One-hundred percent protection of an infrastructure is virtually impossible. Detection capabilities must drastically improve, along with crisis response and mitigation. These capabilities are fundamental to any indications and warnings system and are especially crucial in IW because protection is so fluid. Finally, not all crisis response and mitigation is technical. A policy for public awareness and education in the event of an information crisis (regionally coordinated in an organization similar to FEMA) might stave off panic, alert the public to measures they could take to assist, and lessen immediate public pressure on government officials to "do something." Such pressure in the history of countering terrorism has resulted in hasty responses of overbearing lawmaking and bloody reprisals.

The past 37 years have shown the United States the paradox that "low-intensity conflict" has posed to the world's mightiest military power. However, it is as yet unclear exactly where rogue IW falls in the spectrum of violence. As stated in the beginning, analogies can be useful, but at a certain point, relying on them for analysis becomes harmful. Although the organizational issues of rogue IW defense and counterterrorism might be similar, this similarity might fail for solutions to other common issues. The unfortunate lesson of terrorism is that as long as the United States is unwilling to cede their liberty to prevent violence, there are no total solutions.

What the United States has achieved based on the lessons of terrorism is improved crisis control and policies that demonstrate an awareness of the complex nature of terrorism: its ability to affect any sector or jurisdiction of a free society and the implications that come with those sobering realities. IW has yet to emerge from its dogmatic stage and still offers more slogans than lessons, yet in retrospect of 37 years of fighting terrorism in a concentrated national and international effort, it is unclear whether an electronic Pearl Harbor would elicit a federal response other than the ad hoc overreactions and short-term task forces that have characterized U.S. counterterrorism policy. Such knee-jerk reactions have the potential to do much greater harm in IW than they have in countering terrorism: heavy-handed, short-sighted, and hasty government measures in the information space might have unintended consequences ranging from stymied economic development to unconstitutional regulation to disastrous technical failures. Preempting a rogue IW attack with a multiagency policy of coordination could save the United States from their adversaries, and it might even save them from themselves.

Fighting Against Random Rogue IW

History shows that terrorism more often than not has little political impact and that when it has an effect, it is often the opposite of the one desired by the terrorists. Terrorism in the 1990s and the present time is no exception. The 1991 assassination of Rajiv Gandhi as he campaigned to retake the prime ministership neither hastened nor inhibited the decline of India's Congress Party. Hamas' and Hezbollah's stepped-up terrorism in Israel undoubtedly influenced the outcome of Israeli elections, and it achieved its immediate objective of setting back the peace process on which Palestine Authority President Yasser Arafat had gambled his future. Is a hard-line Likud government really in these groups' best interests? On the other side, Yigal Amir, the right-wing orthodox Jewish student who assassinated Prime Minister Yitzhak Rabin in 1996 because he disapproved of the peace agreement with the Palestinians, might well have helped elect Rabin's dovish second-in-command, Shimon Peres to a full term had the Muslim terrorists not made Israeli security an issue again.

Terrorists caused disruption and destabilization in other parts of the world, such as Sri Lanka, where economic decline has accompanied the war between the government and the Tamil Tigers. However, in Israel and in Spain, where Basque extremists have been staging attacks for decades, terrorism has had no effect on the economy. Even in Algeria, where terrorism has exacted the highest toll in human lives, Muslim extremists have made little headway since 1993, when many predicted the demise of the unpopular military regime.

Some argue that terrorism must be effective because certain terrorist leaders have become president or prime minister of their country. In those cases, however, the terrorists had first forsworn violence and adjusted to the political process. Finally, the common wisdom holds that terrorism can spark a war or, at least, prevent peace. That is true, but only where there is much inflammable material: as in Sarajevo in 1914, so in the Middle East and elsewhere today. Nor can one ever say with certainty that the conflagration would not have occurred sooner or later in any case.

Nevertheless, terrorism's prospects, often overrated by the media, the public, and some politicians, are improving as its destructive potential increases. This has to do both with the rise of groups and individuals that practice or might take up terrorism and with the weapons available to them. The past few decades have witnessed the birth of dozens of aggressive movements espousing varieties of nationalism, religious fundamentalism, fascism, and apocalyptic millenarianism, from Hindu nationalists in India to neofascists in Europe and the developing world, to the Branch Davidian cult in Waco, Texas. The earlier fascists believed in military aggression and engaged in a huge military buildup, but such a strategy has become too expensive even for superpowers. Now, mail-order catalogs tempt militants with readily available, far cheaper, unconventional as well as conventional weapons—the poor man's nuclear bomb, Iranian President Ali Akbar Hashemi Rafsanjani called them.

In addition to nuclear arms, the weapons of mass destruction include biological agents and man-made chemical compounds that attack the nervous system, skin, or blood. Governments have engaged in the production of chemical weapons for almost a century and in the production of nuclear and biological weapons for many decades, during which time proliferation has been continuous and access ever easier. The means of delivery (ballistic missiles, cruise missiles, and aerosols) have also become far more effective. While in the past missiles were deployed only in wars between states, recently they have played a role in civil wars in Afghanistan and Yemen. Use by terrorist groups would be but one step further.

Until the 1970s, most observers believed that stolen nuclear material constituted the greatest threat in the escalation of terrorist weapons, but many now think the danger could lie elsewhere. An April 2000 DoD report says that "most terrorist groups do not have the financial and technical resources to acquire nuclear weapons but could gather materials to make radiological dispersion devices and some biological and chemical agents." Some groups have state sponsors that possess or can obtain weapons of the latter three types. Terrorist groups themselves have investigated the use of poisons since the 19th century. The Aum Shinrikyo cult staged a poison gas attack in March 1995 in the Tokyo subway; exposure to the nerve gas sarin killed 10 people and injured 5,000. Other, more amateurish attempts in the United States and abroad to experiment with chemical substances and biological agents for use in terrorism have involved the toxin that causes botulism, the poisonous protein rycin (twice), sarin (twice), bubonic plague bacteria, typhoid bacteria, hydrogen cyanide, vx (another nerve gas), and possibly the Ebola virus.

To Use or Not to Use?

If terrorists have used chemical weapons only once and nuclear material never, to some extent the reasons are technical. The scientific literature is replete with the technical problems inherent in the production, manufacture, storage, and delivery of each of the three classes of unconventional weapons.

The manufacture of nuclear weapons is not that simple, nor is delivery to their target. Nuclear material, of which a limited supply exists, is monitored by the UN-affiliated International Atomic Energy Agency. Only governments can legally procure it, so even in this age of proliferation, investigators could trace those abetting nuclear terrorists without great difficulty. Monitoring can overlook a more primitive nuclear weapon: nonfissile but radioactive nuclear material. Iranian agents in Turkey, Kazakhstan, and elsewhere are known to have tried to buy such material originating in the former Soviet Union.

Chemical agents are much easier to produce and obtain, but not so easy to keep safely in a stable condition; their dispersal depends largely on climatic factors. The terrorists behind the 1995 attack in Tokyo chose a convenient target where crowds of people gather, but their sarin was apparently dilute. The biological agents are far and away the most dangerous: they could kill hundreds of thousands of people, whereas chemicals might kill only thousands. They are relatively easy to procure, but storage and dispersal are even trickier than for nerve gases. The risk of contamination for the people handling them is high, and many of the most lethal bacteria and spores do not survive well outside the laboratory. Aum Shinrikyo reportedly released anthrax bacteria (among the most toxic agents known) on two occasions from a building in Tokyo without harming anyone.

Given the technical difficulties, terrorists are probably less likely to use nuclear devices than chemical weapons and least likely to attempt to use biological weapons. Difficulties could be overcome, however, and the choice of unconventional weapons will in the end come down to the specialties of the terrorists and their access to deadly substances.

The political arguments for shunning unconventional weapons are equally weighty. The risk of detection and subsequent severe retaliation or punishment is great, and although this may not deter terrorists, it may put off their sponsors and suppliers. Terrorists eager to use weapons of mass destruction may alienate at least some supporters, not so much because the dissenters hate the enemy less or have greater moral qualms, but because they think the use of such violence counterproductive. Unconventional weapon strikes could render whole regions uninhabitable for long periods. Use of biological arms poses the additional risk of an uncontrollable epidemic. And although terrorism seems to be tending toward more indiscriminate killing and mayhem, terrorists may draw the line at weapons of superviolence likely to harm both foes and large numbers of relatives and friends, for example, Kurds in Turkey, Tamils in Sri Lanka, or Arabs in Israel.

Furthermore, traditional terrorism rests on the heroic gesture, on the willingness to sacrifice one’s own life as proof of one’s idealism. There is not much heroism in spreading botulism or anthrax. Because most terrorist groups are as interested in publicity as in violence, and because publicity for a mass poisoning or nuclear bombing would be far more unfavorable than for a focused conventional attack, only terrorists who do not care about publicity will even consider the applications of unconventional weapons.

Broadly speaking, terrorists will not engage in overkill if their traditional weapons (the submachine gun and the conventional bomb) are sufficient to continue the struggle and achieve their aims, but the decision to use terrorist violence is not always a rational one; if it were, there would be much less terrorism, because terrorist activity seldom achieves its aims. What if, after years of armed struggle and the loss of many of their militants, terrorist groups see no progress? Despair could lead to giving up the armed struggle or to suicide. It might also lead to a last desperate attempt to defeat the hated enemy by arms not tried before. Their only hope lies in their despair.

Post Apocalypse

Terrorist groups traditionally contain strong quasi-religious, fanatical elements, for only total certainty of belief (or total moral relativism) provides justification for taking lives. That element was strong among the prerevolutionary Russian terrorists and the Romanian fascists of the Iron Guard in the 1930s, as it is among today's Tamil Tigers. Fanatical Muslims consider the killing of the enemies of God a religious commandment and believe that the secularists at home as well as the State of Israel will be annihilated because it is Allah's will. Aum Shinrikyo doctrine held that murder could help both victim and murderer to salvation. Sectarian fanaticism has surged during the past decade, and, in general, the smaller the group, the more fanatical the group.

As humankind survived the end of the second millennium of the Christian era, apocalyptic movements failed to rise to the occasion. Nevertheless, the belief in the impending end of the world is probably as old as history, but for reasons not entirely clear, sects and movements preaching the end of the world gain influence toward the end of a century, and all the more at the close of a millennium. Most of the preachers of doom do not advocate violence, and some even herald a renaissance, the birth of a new kind of man and woman. Others, however, believe that the sooner the reign of the Antichrist is established, the sooner this corrupt world will be destroyed and the new heaven and earth foreseen by St. John in the Book of Revelation, Nostradamus, and a host of other prophets will be realized.

Extremist millenarians would like to give history a push, helping create world-ending havoc replete with universal war, famine, pestilence, and other scourges. Those who subscribe to such beliefs number in the millions. They have their own subcultures, produce books and CDs by the thousands, and have built temples and communities of whose existence most of their contemporaries are unaware. They have substantial financial means at their disposal. Although the more extreme apocalyptic groups are potentially terrorist, intelligence services have generally overlooked their activities; hence, the shock over the subway attack in Tokyo and Rabin's assassination, to name but two recent events.

Apocalyptic elements crop up in contemporary intellectual fashions and extremist politics as well. For instance, extreme environmentalists, particularly the so-called restoration ecologists, believe that environmental disasters will destroy civilization as they know it (no loss, in their view) and regard the vast majority of human beings as expendable. From such beliefs and values, it is not a large step to engaging in acts of terrorism to expedite the process. If the eradication of smallpox upset ecosystems, why not restore the balance by bringing back the virus? The motto of *Chaos International*, one of many journals in this field, is a quotation from Hassan I. Sabbah, the master of the Assassins, a medieval sect whose members killed Crusaders and others in a religious ecstasy: everything is permitted, the master says. The premodern world and postmodernism meet at this point.

Future Shock

Scanning the contemporary scene, one encounters a bewildering multiplicity of terrorist and potentially terrorist groups and sects. The practitioners of terrorism, up to the present time, were nationalists and anarchists, extremists of the left and the right, but the new age has brought new inspiration for the users of violence.

In the past, terrorism was almost always the province of groups of militants that had the backing of political forces such as the Irish and Russian social revolutionary movements of 1900. In the future, terrorists will be individuals or like-minded people working in very small groups (like the 9-11 terrorists), on the pattern of the technology-hating Unabomber, who apparently worked alone sending out parcel bombs for over two decades, or the perpetrators of the 1995 bombing of the federal building in Oklahoma City. An individual may possess the technical competence to steal, buy, or manufacture the weapons he or she needs for a terrorist purpose; he or she may or may not require help from one or two others in delivering these weapons to the designated target. The ideologies such individuals and minigroups espouse are likely to be even more aberrant than those of larger groups. Terrorists working alone or in very small groups will be more difficult to detect (like the 9-11 terrorists) unless they make a major mistake or are discovered by accident.

Thus, at one end of the scale, the lone rogue terrorist has appeared, and at the other, state-sponsored terrorism is quietly flourishing in these days when wars of aggression have become too expensive and too risky. As we begin a new century, terrorism is becoming the substitute for the great wars of the 1800s and early 1900s.

Proliferation of the weapons of mass destruction does not mean most terrorist groups are likely to use them in the foreseeable future, but some almost certainly will, in spite of all the reasons not to. Governments, however ruthless, ambitious, and ideologically extreme, will be reluctant to pass on unconventional weapons to terrorist groups over which they cannot have full control; the governments may be tempted to use such arms themselves in a first strike, but it is more probable that they would employ them in blackmail than in actual warfare. Individuals and small groups, however, will not be bound by the constraints that hold back even the most reckless government.

Society has also become vulnerable to a new kind of terrorism in which the destructive power of both the individual terrorist and terrorism as a tactic are infinitely greater. Earlier terrorists could kill kings or high officials, but others only too eager to inherit their mantle quickly stepped in. The advanced societies of today are more dependent every day on the electronic storage [6], retrieval, analysis, and transmission of information. Defense, the police, banking, trade, transportation, scientific work, and a large percentage of the government's and the private sector's transactions are online. That exposes enormous vital areas of national life to mischief or sabotage by any computer hacker, and concerted sabotage could render a country unable to function. Hence, the growing speculation about infoterrorism and cyberwarfare.

An unnamed U.S. intelligence official has boasted that with $6 billion and 70 capable hackers, he could shut down America. What he could achieve, a terrorist could too. There is little secrecy in the wired society, and protective measures have proved of limited value: teenage hackers have penetrated highly secret systems in every field. The possibilities for creating chaos are almost unlimited even now, and vulnerability will almost certainly increase. Terrorists' targets will change: why assassinate a politician or indiscriminately kill people when an attack on electronic switching will produce far more dramatic and lasting results? The switch at the Culpeper, Virginia, headquarters of the Federal Reserve's electronic network, which handles all federal funds and transactions, would be an obvious place to hit. If the new terrorism directs its energies toward IW, its destructive power will be exponentially greater than any it wielded in the past—greater even than it would be with biological and chemical weapons.

Still, the vulnerability of states and societies will be of less interest to terrorists than to ordinary criminals and organized crime, disgruntled employees of big corporations, and, of course, spies and hostile governments. Electronic thieves, whether engaged in credit card fraud or industrial espionage, are part of the system, using it rather than destroying it; its destruction would cost them their livelihood. Politically motivated terrorist groups, above all separatists bent on establishing states of their own, have limited aims. The Kurdish Workers Party, the IRA, the Basque ETA, and the Tamil Tigers want to weaken their enemies and compel them to make far-reaching concessions, but they cannot realistically hope to destroy them. It is also possible, however, that terrorist groups on the verge of defeat or acting on apocalyptic visions may not hesitate to apply all destructive means at their disposal.

All that leads us well beyond terrorism as has the military has known it. New definitions and new terms may have to be developed for new realities, and intelligence services and policy makers must learn to discern the significant differences among terrorists' motivations, approaches, and aims. The Bible says that when the Old Testament hero Samson brought down the temple, burying himself along with the Philistines in the ruins, "the dead which he slew at his death were more than he slew in his life." The Samsons of a society have been relatively few in all ages. But with the new technologies and the changed nature of the world in which they operate, a handful of angry Samsons and disciples of apocalypse would suffice to cause havoc. Chances are that of 100 attempts at terrorist superviolence, 99 would fail, but the single successful one could claim many victims, as on 9-11, do more material damage, and unleash far greater panic than anything the world has yet experienced.

The Menace of Amateur Rogue IW

According to DoD government analysts, with a member base of 79,000, the amateur rogue CyberArmy (hackers) may have the biggest armament the Net has ever seen, rallying to take down Web sites that "abuse" the World Wide Web—and removing power from governments. Some missions include hunting for, and taking down, child pornography Web sites.

The CyberArmy wants to regulate the Internet so that the government doesn't come in and regulate it. The CyberArmy started off as a small group of advocates promoting free speech and Internet deregulation. Growing to a full size army of "Netizens," the group has since shifted its views—because of privacy issues and government intervention. Now they believe in Internet self-regulation. If you deregulate, you end up with anarchy. In other words, the CyberArmy is set up just like a game. Members have to solve puzzles (which is usually breaking codes and encryption) to move on to the next commanding level.

Commanding ranks give a member more power and involvement in the organization's missions. Some missions include hunting for, and taking down, child pornography Web sites. The commanding structure begins at the bottom with troopers, rising through the ranks of 2nd Lieutenant, Lieutenant, Captain, Major, Lt. Colonel, Colonel, General, and Marshal. Each division within CyberArmy has its own job to complete, with one of the divisions devoted solely to child pornography Web sites.

This division has taken down about four dozen child porn sites in the last few years, and was also instrumental in bringing down the Wonderland Club child porn ring recently. The group is an advocate of ordinary citizens policing the Internet. Because the Internet is global, governments aren't the right authority to police it.

Hacktivists

In defending the "hacktivist" title that the CyberArmy group has been branded with, the group doesn't believe in defacing a Web site just for the fun of it. If a site is defaced it's usually in the form of protest.

The group was a bit more "hackerish" in 2000—they were considered an amateur menace for a time. However, they're moving away from that. There are more social minded people on the Net now, which is good. Many people join CyberArmy because they are sick and tired of child pornography and Net censorship. CyberArmy's mission is to prove that there are good hackers, not just Script Kiddies. The CyberArmy site also posts discussion boards and Internet tools for users and has a section dedicated to teaching network security.

SUMMARY

The problem of defending against an IW arsenal and tactics is real. U.S. citizens and the organizations that provide them with the vital services they need can find no sanctuary from these attacks. The low cost of mounting these attacks has enlarged the field of potential adversaries and complicated efforts to collect intelligence and array U.S. military defenses. The consequences of a well-planned and coordinated attack by a relatively sophisticated foe could be serious. Even the threat of such an attack or digital blackmail is a distinct possibility. How the public will respond to the threat of IW infrastructure attacks or to actual attacks is unclear but will be a major determinant of future policy and actions.

This situation is getting worse with the rapid proliferation of information technology and know-how. U.S. citizens are becoming increasingly dependent on automation in every aspect of their lives. As information technology becomes an essential part of the way organizations and individuals create products and provide services, the need for interconnectivity and interoperability increases. With this increased need for exchanges of information (and products), vulnerabilities increase. Finally, the increased reliance on commercial off-the-shelf products or commercial services makes it more and more difficult for organizations and individuals to control their own security environment.

Given this situation, you need to focus on two goals. First, you need to find a way to protect yourself against catastrophic events. Second, you need to build a firm foundation upon which you can make steady progress by continually raising the cost of mounting an attack and mitigating the expected damage of the IW arsenal and tactics of the military. The conclusions are as follows.

Conclusions

- Information warfare (IW) has become virtually synonymous with the revolution in information technologies and its potential to transform military strategies and capabilities.
- There is a growing consensus that national prosperity, if not survival, depends on one's ability to effectively leverage information technology. Without being able to defend vital information, information processes, and information systems, such a strategy is doomed to failure.
- IW is often thought of as being defined by a particular target set of decision makers, information, information processes, and information systems.
- The battlespace associated with IW has been a constantly expanding one, moving far beyond traditional military situations.
- In some quarters, IW has even been associated with the leveraging of information technologies to achieve greater effectiveness and efficiency. This has stretched the meaning of IW to the breaking point and has sowed more confusion than enlightenment. For this reason, this treatment of the subject uses the term *information strategies* to refer to the recognition and utilization of information and information technologies as an instrument of national power that can be independent of, or complementary to, military presence and operations.

- The scope, or battlespace, of information warfare and strategy (IWS) can be defined by the players and three dimensions of the nature of their interactions, the level of their interactions, and the arena of their interactions.
- Nation-states or combinations of nation-states are not the only players. Nonstate actors (including political, ethnic, and religious groups; organized crime; international and transnational organizations; and even individuals empowered by information technology) are able to engage in information attacks and to develop information strategies to achieve their desired ends.
- The term *war* has been used so loosely in recent times (War on Poverty, War on Drugs, War on Crime) that it should be no surprise that IW has evolved over the past several years to become a catch-all term that encompasses many disparate activities, some of which have long been associated with competition, conflict, and warfare, and others that are of more recent origin. These include activities that range from propaganda campaigns (including Media War), to attacks (both physical and nonphysical) against commanders, their information sources, and the means of communicating with their forces.
- Under this rather large umbrella that has become known as IW, one can find activities long associated with military concepts and operations, including deception, command and control warfare (C2W), and psychological operations (psyops).
- Technological advances have added new forms such as electronic warfare (EW) and "hacker warfare."
- The term *defensive information warfare* (IW-D) is used here to refer to all actions taken to defend against information attacks, that is, attacks on decision makers, the information and information-based processes they rely on, and their means of communicating their decisions.
- Strictly speaking, because these attacks can be launched during peacetime at nonmilitary targets by nonmilitary groups, both foreign and domestic, the term IW-D should be IWS-D. However, IW-D is currently in wide use.
- This overview of IW-D does not attempt to deal with the problems of defending against all of the different kinds of information attacks, but rather focuses its attention on the subset of IW that involves attacks against information infrastructure, including what has become known as "hacker warfare" and in its more serious form, "digital warfare."

An Agenda for Action

The cornerstone of the military's efforts to combat IW will be the efforts of all global military organizations to protect their own systems and information. Some military organizations have been worrying about this for a long time and have developed and implemented plans to keep on top of this increasingly serious set of threats. Other military organizations have more work to do. It might be helpful, even for those military organizations that feel they are well prepared, to review the list of suggested action steps to determine what they need to do to be better prepared for the future.

The United States government needs to set an agenda for action that goes beyond the work already done in preparation for the IW arsenal and tactics of the military. With the preceding in mind, when completing the Information Warfare Arsenal and Tactics of the Military Checklist (Table F14.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for networks. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Information warfare (IW) has not become synonymous with the revolution in information technologies and its potential to transform military strategies and capabilities.
2. True or False? There is a lessening consensus that national prosperity, if not survival, depends on one's ability to effectively leverage information technology.
3. True or False? Information warfare is often thought of as being defined by any target set of decision makers, information, information processes, and information systems.
4. True or False? The scope, or battlespace, of information warfare and strategy (IWS) can be defined by the players and three dimensions of the nature of their interactions, the level of their interactions, and the arena of their interactions.
5. True or False? The battlespace associated with IW has been a constantly expanding one, moving far beyond traditional military situations.

Multiple Choice

1. Which one of the following is not an individual element of C2W, covering both offensive and defensive applications?

A. Operations security
B. Commercial deception
C. Psychological operations
D. Electronic warfare
E. Targeting

2. In light of the IW arsenal and tactics analysis of the military, the following overall sustained terrorist IW tactics observations stand out, except one:

A. Terrorism
B. Geopolitics of terrorism
C. Counterterrorism versus new terrorism
D. U.S. exposure
E. General counterterrorism strategy

3. A core, longer-term strategy must do the following, except:

A. Attempt to deal with the problems of defending against all of the different kinds of information attacks
B. Address the political, economic, and social roots of international terrorism
C. Make deterrence relevant to non-state actors as well as state sponsors
D. Reduce the risk of truly catastrophic terrorism using weapons of mass destruction

4. DoD has also articulated a similar concept for an office within the Executive Office of the President, organized for countering terrorism, as a potential focal point for the oversight of the U.S. antiterrorist program. This office would be a permanent body with a White House perspective; such a staff could perform the following, except one:

A. Monitor and coordinate activities of the line agency and departments.
B. Identify unneeded capabilities.
C. Identify special resources that might be mobilized if an international incident occurs.
D. Pull together current intelligence and ongoing analysis and research efforts.
E. Identify terrorist incidents.

5. Nation-states or combinations of nation-states are not the only players. Which of the following non-state actors is not able to engage in information attacks or develop information strategies to achieve their desired ends?

A. Political, ethnic, and religious groups
B. Organized crime
C. Law enforcement organizations
D. International and transnational organizations
E. Individuals empowered by information technology

Exercise

The board of directors of a technical research company demoted the company's founder and chief executive officer. The executive, disgruntled because of his demotion, was later terminated; it was subsequently determined that the executive had planned to quit about the same time he was fired and establish a competitive company. Upon his termination, the executive took home two computers; he returned them to the company five days later, along with another company computer that he had previously used at home. Suspicious that critical information had been taken; the company's attorneys sent the computers to a CFS team (CFST) for examination. How did the CFST go about conducting the forensics examination?

HANDS-ON PROJECTS

A senior member of a major organization was under suspicion of downloading thousands of pornographic images from the Internet. He strongly denied it all, but the case against him looked very grim. How did the CFS go about conducting the investigation?

Case Project

A major high-tech company took-over a smaller subsidiary in a related, but non-competing, business area. The smaller company was merged into the larger as a new business unit. Most of the previous management team was bought-out and left the company; others were persuaded to stay on to manage the new subsidiary. Two years later, the individuals who left had already started another company in the same market segment as their old company, in possible breach of the buy-out agreement. Business results of the new subsidiary had simultaneously begun to deteriorate. The CEO of the new subsidiary, (who had originally held the same position in the bought-out company) renegotiated a new contract, under highly favorable conditions, and then immediately resigned, triggering certain beneficial clauses in the contract. How did the CFST go about conducting their examination?

Optional Team Case Project

An insurance company was contesting a claim for $400,000 for loss of all data from a company's central computer. The computer had allegedly been flattened by a large industrial magnet and all the data had disappeared from the hard disk. How was the CFST able to help the insurance company?

REFERENCES

[1] Vacca, John R., *Firewalls: Jumpstart for Network and Systems Administrators,* Elsevier Digital Press, Burlington, MA, 2004.

[2] Vacca, John R., *Wireless Broadband Networks Handbook*, McGraw-Hill, New York, 2001.

[3] Vacca, John R., *High-Speed Cisco Networks: Planning, Design, and Implementation*, CRC Press, Boca Raton, FL, 2002.

[4] Vacca, John R., *Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan*, McGraw-Hill, New York, 2001.

[5] Vacca, John R., *Satellite Encryption*, Academic Press, New York, 1999.

[6] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

This page intentionally left blank

15 The Information Warfare Arsenal and Tactics of Terrorists and Rogues

The information warfare (IW) arsenal and tactics of terrorists and rogues have become increasingly transnational as the networked organizational form has expanded. When terrorism's mentors were the Soviet Union and the Eastern Bloc, they imposed their own rigid hierarchical structure on terrorist groups. Now that terrorism is increasingly substate, or semidetached, networking and interconnectivity are necessary to find allies and influence others, as well as to effect command and control.

As discussed in Chapter 14, information and communication technologies (ICTs) have facilitated this and have enabled multiple leaders to operate parallel to one another in different countries. It therefore might be said that a shift is taking place from absolute hierarchies to hydra-headed networks, which are less easy to decapitate. An analogy, using the Palestinian example, may be that the more networked form of Hamas now that Arafat is dead, is replacing the hierarchical structure of the PLO. In many ways the Afghan War was a seminal event in promoting the networked form in that it showed that fluidly organized groups, driven in this case by a religious imperative, could defeat an experienced hierarchically structured army.

Geographical dispersion, both physical and in cyberspace, provides extra security. A rigid hierarchical structure is more easily penetrated and neutralized. Israel's admission that it had not yet found a way to deal with Hamas's decentralized and internationalized command and control structure, which uses encrypted Internet messages, suggests it has had difficulty in this matter. An investigation by the Federal Bureau of Investigation into terrorist activity in the United States indicated that part of Palestinian Islamic Jihad's command and control system was located in Tampa, Florida. Likewise, Hamas allegedly has some of its fundraising infrastructure in London and the United States and publishes its main Arabic journal, *Filistin al Muslima,* in London.

Islamist terrorists may be said to fit the network ideal. Many supportive expatriate communities are based in sympathetic or neutral states, enabling political activists and terrorists to operate within the safe haven that modern democracies provide.

NOTE

It is not the intention here that the term "Islamists" should refer only to terrorist organizations, but rather to those Muslim militants who believe that Islam is incomplete without its own state, one in which Shariah provides the system of governance, and who campaign for its imposition.

Among Islamists, it is the Jihadists (religious warriors) who are of particular interest in this chapter. The followers of Hasan al Banna, Sayyid Qutb, and Abdul Ala Maududi, the organizations they founded, Ikhwan al Muslimoon and Jamaat Islami, and the ideological off-shoots these have spawned, give rise to the Jihadist ideology. Although the concept of Jihad may be interpreted on different levels, it often incorporates violence when applied to Islamists.

NOTE

The ultimate experience is, of course, Jihad, which for Islamists means armed battles against communists (Afghanistan) or Zionists (Palestine and Israel) or, for the radicals, against renegades and the impious.

Jihad in the modern Islamist sense knows no political space or state; its space is that of the Umma, the community of Muslims, wherever they may be. An example of the networked form among such Islamist organizations is that of the Algerian Armed Islamic Group, the GIA. Allegedly responsible for a bombing campaign in France, it appears to have had a command and control center in Britain for some years prior to the expulsion of some members by the British authorities. At the same time, sympathizers were also safe-housing some of its weapons and explosives in Belgium.

Algerian terrorists have been able to communicate with their sympathizers and members by use of the Internet and have used the services of Muslim news agencies, which republish their postings. Foremost among them is MSANEWS. On their site were published communiqués from the GIA, Front Islamique de Salut (FIS), and many other Islamists.

NOTE

The MSANEWS also posts articles and communiqués from non-Islamist Muslim and non-Muslim sources, claiming that it has condemned terrorism and that it no longer reposts communiqués of organizations that advocate terrorism.

The site of the Campaign for the Defense of Legitimate Rights (CDLR), the Saudi opposition group, also contains postings from groups not directly connected with it, as do London-net@Muslimsonline and the pro-Iranian Muslimedia International, which, like other sites, reposts interviews with Osama bin Laden, the exiled and wanted *dead or alive* Saudi terrorist leader (see sidebar, "Bin Laden Uses Web to Plan"). As with some other Islamist groups, Muslimedia International also promotes antisemitism and Holocaust denial and provides links with the American Holocaust denier, Michael Hoffman II and his Campaign for Radical Truth in History, thereby highlighting the interconnectivity possibilities between totally different ideologies sharing a perceived common enemy.

BIN LADEN USES WEB TO PLAN

Osama bin Laden and other Muslim extremists are using the Internet to plan more terrorist activities against the United States and its allies. Recently, U.S. law enforcement officials and other experts disclosed details of how extremists hide maps and photographs of terrorist targets in sports chat rooms and on pornographic bulletin boards and other popular Web sites. Instructions for terrorist activities also are posted on the sites, which the officials declined to name. To a greater and greater degree, terrorist groups, including Hezbollah, Hamas, and bin Laden's al Qaeda, are using computerized files, email, and encryption to support their operations—like the train bombing in Madrid in the winter of 2004. According to various unnamed officials and investigators, the messages are scrambled using free encryption programs set up by groups that advocate privacy on the Internet. It's something the intelligence, law-enforcement, and military communities are struggling to deal with. The operational details and future targets, in many cases, are hidden in plain view on the Internet. Only the members of the terrorist organizations, knowing the hidden signals, are able to extract the information.

An Islamist site that particularly aims its message to the outside world is that of Hizb-ut-Tahrir, the Islamic Liberation Party. Their first U.K.-based site was hosted by Imperial College, London, but following complaints to the college authorities, the site was closed down. They now post in their own name as Hizb-ut-Tahrir, and as Khilafah, providing Internet-based access to their hard copy material, literature, and their regional activities. Al-Muhajiroun (The Emigrants) whose U.K. leader, Omar Bakri Mohammed, was the founding leader of Hizb-ut-Tahrir in Britain, and from which he split claiming differences with the Middle-East-based leadership, also provides details of its activities, as well as lists of its hardcopy publications and contacts. In 1998, Mohammed reported the communiqués of Osama bin Laden, for whom he claims to act as a spokesman. As a consequence of his endorsement of the bombings of the U.S. embassies in Dar-es-Salaam and Nairobi, his postings are no longer carried by MSANEWS.

Hamas and its supporters and sympathizers have been among the most prolific users of the Internet. MSANEWS provides a list of Internet resources about Hamas, including copies of its covenant, its official communiqués (at Assabeel On-line), and communiqués of its military wing, the Izz al-Din Al-Kassam Brigades. Information about Hamas may also be accessed in various different ways: via MSANEWS, the Palestine site, and the Islamic Association for Palestine. Hamas' own site, which posts in Arabic, is the Palestine Information Centre.

Religious luminaries from one country sometimes act as the higher legal and moral authority in another country. Sheikh Yusuf al-Qaradawri of the Egyptian Ikhwan al-Muslimoon (Muslim Brotherhood) lives in Qatar and serves as the Imam (religious leader) for the Palestinian Hamas. Sheikh Ibn Qatada, a Jordanian Palestinian living in London, serves as the Imam for the Algerian GIA. Sheikh Abu Hamza, an Egyptian national and former Afghan Jihad volunteer, serves as a propagandist for the Algerian GIA and Imam for the Yemeni Jihad group but lives in London. Now, their messages of guidance and support find an outlet most frequently via ICTs.

Although some commentators have argued that modern cultural forces, such as ICTs, serve to undermine Islamization in Muslim society, it is equally easy to argue that they provide a new and growing medium by which Islamism is disseminated. Even if they do not reach the poorer sections of Muslim society, they certainly reach many educated expatriate communities among whom they find support. The growing number of advertisements, on the Internet and in Muslim papers and journals, for conferences to discuss the use of the Internet to promote Islam, or Islamism, supports the thesis that many activists and religious teachers see these developments as positive ones to be recommended and encouraged.

Combining religious injunctions with strategic commands is a feature of such Islamist leaders and their groups. Calls to carry out Jihad are frequently cloaked in religious and pseudo-religious language, but the implication is clear for the target audience. Thus, for example, Osama bin Laden's *Ladenese Epistle,* which was originally faxed to his London contact, Khalid al Fawaz and then posted to MSANEWS in August 1996 by the London-based Saudi dissident groups CDLR and MIRA, is recognized as providing general guidance for anti-American terrorism. For example, bin Laden's *Ladenese Epistle* reads,

> The sons of the land of the two Holy Places had come out to fight against the Russian in Afghanistan, the Serb in Bosnia-Herzegovina, and today they are fighting in Chechenia and—by the Permission of Allah—they have been made victorious over your partner, the Russians. By the command of Allah, they are also fighting in Tajakistan.

> I say: Since the sons of the land of the two Holy Places feel and strongly believe that fighting (Jihad) against the Kuffar in every part of the world, is absolutely essential; then they would be even more enthusiastic, more powerful and larger in number upon fighting on their own land.

The Nida'ul Islam site, based in Australia, promotes an uncompromising message of both Jihad and of suicide terrorism. A recent posting, "The Islamic Legitimacy of the Martyrdom Operations," states that martyrdom is forbidden in Islam, but cites approvingly those martyrs who willingly gave their lives for Muslim causes and then transposes these causes to contemporary issues. It attempts to demonstrate with quotes from the Quran and the Sunnah that Islamic bombing assaults and martyrdom attacks are legitimate and fall within the framework of Islam.

Azzam Publications, named after Abdullah Azzam, a Palestinian who became a military leader in Afghanistan and who was assassinated in Pakistan in 1989, has also published calls for Jihad volunteers:

> The Saudi Government does not intend to help the Muslims in Kosova and it has prevented its nationals from going there to fight. This means that the Jihad in Kosova is now a greater responsibility on Muslims with western nationalities... Redistribute this e-mail message all over the world...telephone the nearest Saudi Embassy or Consulate to protest against this crack-down and tell everyone to do so until it jams the lines of the Saudi Consulates around the world...e-mail the Saudi Embassy in Washington with messages of protest...begin to prepare yourselves to go and fight in Kosova to make up for the lack of manpower that was heading there from Saudi Arabia. Wait for the Kosova bulletin from Azzam Publications.

Among the far right, the U.K.-based national revolutionary group, The International Third Position, illustrates graphically the adoption of ICTs to enhance a position. The group is tiny, but its foreign contacts are numerous, widespread and growing. In just over one year its *Final Conflict* email newsletter has grown in size and scope to reflect the news of, and messages from, its worldwide contacts.

Final Conflict also acts as a news agency for Holocaust deniers (in much the same way as MSANEWS does for Islamists), many of whom are also far right extremists. For example, the email newsletter reposts communiqués from David Irving and Fredrick Toben's Australian Adelaide Institute, which like the California-based Institute for Historical Review, attempts to provide a scholarly veneer for denial. Some invitees to a conference held by the Adelaide Institute were refused permission to visit Australia by its Department of Immigration, but the easy access to the Internet and video links facilitated conference presentations that otherwise might not have taken place.

The far right has also used the Internet to post bomb-making manuals that are not otherwise available in Europe. The British neo-Nazi, David Myatt, of the National Socialist Movement posted his *Practical Guide to Aryan Revolution* in November 1997 at the Web site of Canadian Bernard Klatt in order to evade police scrutiny. The chapter headings included: "Methods of Covert Direct Action," "Escape and Evasion," "Assassination," "Terror Bombing," "Sabotage," "Racial War," "How to Create a Revolutionary Situation," "Direct Action Groups," and so on. The contents provided a detailed step-by-step guide for terrorist insurrection with advice on assassination targets, rationales for bombing and sabotage campaigns, and rules of engagement. Although he may have committed no indictable offence in Canada, Klatt was forced to close down his site in April 1998. Myatt is currently the subject of a British criminal investigation for incitement to murder and promotion of race hatred.

Police forces in Britain and France recently investigated an international neo-Nazi network that issued death threats against French celebrities and politicians from their British-based Internet site. Herve Guttuso, the French leader of the Charlemagne Hammer Skins, was arrested in Essex at the same time as eight members were arrested in the South of France. The French members of the network were charged with making death threats, and Guttuso was the subject of a French extradition request to the British courts. According to the French Interior Ministry, police in Toulon traced the London address of the Internet site, which was being accessed about 7,000 times a month. The investigation enabled the police to identify 3,500 people sympathetic to the neo-Nazi group in various countries including Britain, Greece, Canada, America, and Poland. The investigators found that the Charlemagne group appeared to be one of the largest and best organized neo-Nazi groups yet uncovered, with a coordinated international structure and logistical centers for disseminating violent racist propaganda, based principally in Britain and America. Although the group gave a postal address in London as their center, their material was disseminated via Klatt's FTC Net (as have been the postings of Marc Lemire, Paul Fromm, Doug Christie, The Heritage Front, and other neo-Nazi and white supremacist groups).

The British far right may have been slower to realize the command and control possibilities of ICTs than their U.S. or German co-ideologies, but they appear to be catching up. Although in recent years it is the violent skinhead music scene that has provided the main medium through which they promote liaison, it is clear that for some the future lies with ICTs.

In 1999, the Pentagon had to admit that there had been a major assault on its computer systems. Zionist Occupational Government (ZOG) observers (or Pentagon observers) have increasingly warned that the frequency and sophistication of the hack attacks will only increase as dissident groups realize that they can strike at the very heart of ZOG at the touch of a few buttons. It doesn't matter what government specialists invent to counter the techno-terrorist; there is always a way around their antihacker programs, and the more ZOG relies on computers, the more damage can be done by attacking their systems.

NOTE

Zionist Occupied (Occupational) Government, or ZOG, is a term used to refer to the belief that the United States government is controlled by "Zionists" where the word "Zionists" is sometimes used as a euphemism for "Jews." Some groups are more direct and refer to the Jewish Occupied Government. The term is often rendered as "Zionist Occupation Government" or even "Zionist Occupational Government."

THE TERRORIST PROFILE

Sid-Ra, a 6-foot-4-inch, 350-pound giant of a man, paces between his "subjects" in the smoke-filled Goth club Click + Drag, located in the old meat-packing district of Manhattan. Inside the club are leather-clad, black-lipped females and young men dressed in women's underwear. Sid is a hacker-terrorist and an acknowledged "social engineer" with curious nocturnal habits. There are thousands of people like him, who by day are system and network administrators, security analysts, and start-up cofounders. When night comes, they transform into something quite different.

Is this the profile of a "wanna-be" terrorist? Perhaps! These are the self-proclaimed freedom fighters of cyberspace. They even have a name for it: hactivism. Political parties and human rights groups are circling around to recruit hactivists into their many causes. Recently, for example, the Libertarian Party set up a table at the HOPE (Hackers on Planet Earth) conference. The San Francisco–based Electronic Frontier Foundation (EFF) collected donations, and members of civil-rights groups, including the Zapatistas, a Mexican rebel group, spoke up at one of two sessions on hactivism.

Even without such civil-liberties groups trying to organize them, hactivists have been busy on their own. They have formed privacy-related software companies such as ZeroKnowledge Systems USA Inc. in Montreal. They're developing anonymous, inexpensive email and Web-hosting services through the DataHaven Project Inc. (*http://www.dhp.com*), and they're trying to get the Internet out to third world human rights organizations through groups such as Cult of the Dead Cow Communications (cDc; *http://www.cultdeadcow.com/*).

CAUTION

URLs are subject to change without notice.

Sid feels hactivism's pull so strongly that he makes a dramatic claim: "The Internet is the next Kent State, and we're the ones who are probably going to get shot."

From Vietnam Marches to Cyberdisobedience

Like any social engineer, Sid exaggerates. Except for the four-year jail terms handed down to Kevin Mitnick and Kevin Poulsen, sentencing for even criminal hacking in 2003–2004 has been relatively light (mostly probation and fines) because of the suspects' young ages.

NOTE

Kevin Mitnick is one of the most famous hackers to be jailed and convicted. Mitnick's last arrest was by the FBI on February 15, 1995—he was charged with breaking into some of the United States' most "secure" computer systems. Kevin Poulsen's hacker handle was "Dark Dante." He worked for SRI International by day, and hacked at night. He trained to be the complete hacker and even taught himself lock picking. Among other things, he reactivated old Yellow Page escort telephone numbers for an acquaintance who then ran a virtual agency. He was finally arrested in April 1991. Poulsen is now a journalist and serves as editorial director for SecurityFocus.

However, the comparison to the psychedelic hippies of the 1960s who spoke out against the Vietnam War may not be so far off the mark—only this time, the hackers are Goths and hedonists, and they're using the Internet to rid the world of tyranny.

The government tries to put electronic activism into the peg of cyberterrorism and crime with its infowar eulogies (IW success stories), but E-Hippies, cDc, and others aren't criminals. The Internet just multiplies their voices. Another group reaching out to hackers and technologists is the EFF. In 1999, the EFF successfully argued in the infamous Bernstein ruling, which stated that software code is protected as a form of speech.

Hackers question conventional models. They don't just look at technology and say, "This is how it works." They say, "How can I make it better?" They look at society that way too—their government, their schools, and their social situations. They say, "I know how to make this better," and they go for it.

In the Motion Picture Association of America (MPAA) case, staffers at 2600 Enterprises Inc., based in Middle Island, New York, were threatened with imprisonment if they didn't remove a link on the 2600 Web site to the code used to crack DVD encryption. Because the link was editorial content, it set Sid off on another diatribe.

The Libertarian Party also recruits hackers and technologists. At HOPE, the party's New York State committee (*http://www.cownow.com*) handed out fliers, signed up recruits, and took a "sticker" poll of party affiliations. The poll got hacked, but about half the stickers were yellow—for libertarian, anarchist, or independent. Many party members are programmers. They're trying to rally hackers around encryption, privacy, and freedom-of-communication planks. Hackers can offer them freedom, because the Internet routes around tyranny.

Hackers have ways beyond the Internet to electronically spread their message. Take a young dude named Alpha Underflow, for instance, who late one night broke the lock to a lit-up roadside-construction sign and reprogrammed it to read, "Hack Planet Earth" in support of the 2600 Magazine staff, but then, he also likes to use his reprogrammed garage-door opener to pop open his neighbor's garage doors.

The Older Generation

This moral confusion is typical of the younger hacking crowd, but most of the older hackers (30 years old and up) have grown up. In the mid-1990s, there was more disillusionment as more bleeding-edge hackers ended up going to jail for cracking. That bummed out their whole theme, but now they've learned some limits and they can still operate within them.

That means the older hackers do develop some scruples. For example, the EFF Web site (*http://www.eff.org*) was a popular target of punk hackers in the mid-1990s, with hacks and defacements occurring weekly. Now it's rarely hacked. When the site did get hacked, a message was posted about it on 2600's bulletin board, and the hackers who responded called that hacker a lamer. The process that turned the hippie of 1968 into the employed investor of 1985 is similarly going on here today. With luck, the hippie-to-yuppie disillusionment won't happen to hackers, too.

Who are the real cyberterrorists? Are they for real?

Will the Real Cyberterrorists Stand Up

The debate over whether the United States faces imminent danger from cyberterrorist attacks took a new turn recently when the National Security Council declared that *terrorism* may be too strong a word when describing potential cyberthreats. Although it would be a tough call to tell the difference between an attack by hackers and one launched by terrorists intent on disrupting national security, the administration's cyberdefense programs are battling a perception problem that stems from the misuse of the word *terrorism*.

Maybe we shouldn't be saying "cyberterrorism." Maybe we should be saying "information warfare." In the end, we're going to know it when we see it—the difference between joy-riding hackers and state-sponsored cyberattacks.

Experts agree that, to date, most of the major cybersecurity incidents are best described as nuisance attacks, although many fear that a devastating surprise attack, sometimes referred to as an "electronic Pearl Harbor," is inevitable. Although the government tries to be proactive, the United States is going to get nailed seriously—sooner rather than later. By not preparing for the worst-case scenario, the United

States may be endangering the public's civil liberties. A lot of people are going to be willing to throw civil liberties out the window in an effort to recover from an attack that cripples large portions of the nation's critical infrastructure.

Preparation is crucial, and, in the current legal system, defensive measures are more "workable" than offensive ones. Overall, however, cyberdefense is not well understood and is not talked about sufficiently. Pretending the threats are not there is not a solution. Rogue groups have made numerous efforts to acquire encryption algorithms and sophisticated tools. One presidential administration after another has lulled the American people into a false sense of security.

The Internet has become a new form of the "dead drop" (a Cold War–era term for where spies left information) for terrorists and, bin Laden, the dissident and wanted Saudi businessman who has been indicted for the 1998 bombing of two U.S. embassies in East Africa, the 9-11 attacks in 2001, the bombing of the *USS Cole* destroyer in Yemen, and the 2004 train bombing in Madrid, Spain, has taken advantage of that Internet dead drop zone.

Four alleged bin Laden associates went on trial recently in federal court in New York for the embassy bombings. Officials say bin Laden began using encryption in 1996 but recently increased its use after U.S. officials revealed they were tapping his satellite [1] phone calls in Afghanistan and tracking his activities.

Thus, bin Laden meets the requirements for the new terrorist profile: he will use whatever tools he can (emails, the Internet, etc.) to facilitate jihad against the Israeli occupiers and their supporters, according to Ahmed Yassin, the founder of the militant Muslim group Hamas. Bin Laden has the best minds working for him.

WHY TERRORISTS AND ROGUES HAVE AN ADVANTAGE IN IW

Governments have neither the financial resources nor the technical know-how to stay on top of hackers and computer terrorists. This is why terrorists and rogues have an advantage in IW. The private sector must itself take much of the action that is necessary to prevent attacks being made on the Internet. It's no longer possible for governments to provide the resources and investment necessary to deal with these kinds of issues.

There are no cookie-cutter solutions; every network is different. At the top of chief information officer's (CIOs) lists of concerns are denial of service (DoS) attacks, which recently brought Yahoo, Amazon.com, eBay, and other high-profile Web sites to their knees. DoS attacks are a key concern because the only way that is currently available to prevent them is to catch the perpetrators.

Second on the list of concerns is attacks that reach into networks to steal valuable corporate data. Firewalls [2] are the best way to prevent data theft that originates outside of a network, whereas cryptography can help protect data from internal theft. There is a real danger of terrorists and hostile rogue nations using computer networks to wage international warfare. In other words, most of the major terrorist organizations have their own Web sites, and therefore have the facility to carry out the same sort of action that was carried out with the release of the "I Love You" virus. Cyberterrorism can be more effective and more costly to governments than the classic methods of bomb attacks and assassination. It is a serious threat to everyone in all societies.

Solutions seem harder to come by today than solutions to the problems just discussed. Governments, businesses, and research institutions must band together to find the best technologies and courses of action to defeat cyber crimes. Companies must be more willing to invest in security systems to protect their networks. A few of these companies called on software companies and service providers to make their products more secure. Default settings for software products sold to consumers should be at the highest level of security. You wouldn't build a swimming pool in the center of town and not put a fence around it. Basically, that's just what the software companies are doing.

Although security firms have financial incentives for promoting security issues, for the average corporation, the benefits of spending millions of dollars to bolster security in networks aren't immediately obvious, thus making them slow to act. If you have a choice of spending five million dollars on getting 693,000 new customers, or five million dollars on better serving the ones you already have, that's a difficult value proposition. Most companies would take the additional customers. The severity of attacks could get worse, though, and businesses would be wise to make precautionary investments now. Most businesses have been lucky so far.

Cyberattack Risks If You're a Superpower

IW and other security threats simply come with the territory when your country is the world's only remaining superpower. This is what is called a "superpower paradox." There is no other country that can challenge the United States directly. Instead, some countries look for indirect ways to challenge the United States. This challenge could come in the form of nuclear (see sidebar, "Stopping Nuclear Blackmail"), chemical, biological (see sidebar, "Chemical and Biological Terrorism"), or even cyberwarfare (see sidebar, "Hacker-Controlled Tanks, Planes, and Warships") attacks.

STOPPING NUCLEAR BLACKMAIL

Bill Clinton used to say that no Russian missiles are targeted at the United States, but there is every reason to believe that there are, or soon will be, North Korean missiles targeted at this country—missiles capable of delivering nuclear or chemical and biological warheads. In a few years, and without much warning, Iranian and Iraqi missiles

→

could also be targeted at us and our allies. What can the United States do to stop such missiles once they are launched? Not a thing.

None of this was clear in 1998; it is undeniable now. The question is whether the U.S. government will build a missile defense system to protect their cities, military bases, and oil fields—and to block the kind of nuclear blackmail suggested by China's threat, during the Taiwan Strait crisis of 1996, to bomb Los Angeles.

A full warning came in a 1998 report of the commission on missile threats headed by Defense Secretary Donald Rumsfeld. This was a bipartisan commission, with members who have often disagreed on weapons issues. The panel had access to all U.S. intelligence sources, and its conclusion was unanimous: rogue states could inflict major destruction on the United States within five years of deciding to do so, and with little or no notice to us.

This contradicted the Clinton administration line that the United States would have plenty of notice of a missile attack. That conclusion was based on a 1995 national intelligence estimate that said there would be no threat to the 48 contiguous states for the next 15 years.

NOTE

Evidently, the administration didn't think that the constitutional obligation to "provide for the common defense" applied to Alaska and Hawaii.

The Rumsfeld report at first seemed to do little to change the views of President Clinton's top defense advisers. Five weeks after the report was released, Gen. Henry Shelton, the chairman of the Joint Chiefs of Staff, wrote that "the intelligence community can provide the necessary warning" of hostile missile development and added, "We view this as an unlikely development." A week after that, North Korea launched a 3,000-kilometer range, two-stage Taepo Dong 1 missile over Japan. The launch indicates that North Korea has made progress in building the Taepo Dong 2, whose 10,000-kilometer range includes not only Alaska and Hawaii but also much of the continental United States. No matter: all but four Senate Democrats blocked action on a bill sponsored by Thad Cochran, a Republican from Mississippi, and Daniel Inouye, a Democrat from Hawaii, that would have forced the administration to deploy a missile defense system as soon as technologically feasible.

A New World

The case against rapid deployment rests on three arguments: (1) the threat isn't real, (2) the technology is impossible, and (3) it is more important to maintain the antiballistic missile treaty signed with the Soviet Union in 1972, which bars most missile defense systems. The Rumsfeld report demolished argument 1. Argument 2 is still raised by some who note that the United States has spent large sums on missile

→

defense since Ronald Reagan proposed it in 1983, with disappointing results, but stopping a few rogue-state missiles with the computers of 2005 is much easier than stopping hundreds of Soviet missiles with the computers of 1983. As for argument 3, the strategic environment in which the antiballistic missile treaty was adopted no longer exists. The argument for the treaty was that a missile defense system might provoke a Soviet or American first strike. However, the proximate missile threats now come from states that might risk such a strike.

CHEMICAL AND BIOLOGICAL TERRORISM

In *For Your Eyes Only*, James Bond's irrepressible quartermaster, Major Boothroyd (a.k.a. Q) demonstrates his latest toy: a rather lethal umbrella. Using a faceless mannequin, one of Q's assistants illustrates how the umbrella looks and acts like it should until struck by water (as umbrellas are wont to do from time to time). Suddenly, sharp metal hooks extend all along the edge of the umbrella as it swiftly closes upon the victim's neck. The motion is quick and precise, but one can't help but imagine the far messier spectacle if a human being were caught under it in a rainstorm.

Unfortunately, the fictional version of MI6 portrayed in the James Bond films is not the only place one can find a deadly device masquerading as protection against the elements. In September 1978, the Bulgarian secret service shot a Bulgarian exile, Georgi Markov, with just such a device. Disguised as an umbrella, the surreptitious gun inserted a small pellet into Markov's thigh. The pellet contained only a few hundred millionths of a gram of the deadly poison ricin (supplied by the KGB), but it was enough. Markov died four days later in a London hospital. Another Bulgarian defector, Vladimir Kostov, was similarly attacked in Paris the month before. Kostov was shot in the back and suffered a high fever, but survived. He sought medical treatment after hearing of Markov's death and doctors removed from his back a small pellet identical to the one used to kill Markov.

Not satisfied with leaving such methods solely in the hands of the secret agent-types, the Aum Shinrikyo cult tried a simpler version during their chemical and biological escapades. In their infamous sarin gas attack on the Tokyo subway, Aum operatives chose the decidedly low-tech dissemination method of dropping bags of liquid sarin on the floor, puncturing them with the sharpened ends of their umbrellas, and then beating a hasty retreat as the nasty stuff spilled out onto the ground. Despite their primitive dissemination methods, Aum managed to murder 12 people, injure over a thousand, terrorize several thousand more, and spark a national weapons of mass destruction counterterrorism industry in the United States.

→

Analysts have long commented on the copycat nature of terrorists and terrorist groups. Once a new method of attack (from car bombings to airplane hijackings to planes being used as bombs to hostage-taking for ransom money) has met with success, other terrorist groups are bound to emulate it. Given such a phenomenon among terrorists, is the United States witnessing any evidence of an increase in the use of umbrellas in terrorist operations—especially those involving chemical and biological weapons? Should the United States be calling for an international embargo on umbrella sales to Afghanistan to prevent Osama bin Laden and his al-Qaeda organization from acquiring such dangerous, dual-use technology? Probably yes.

For one thing, Aum has inspired many follow-up attacks that analysts had predicted shortly after their March 1995 attack. Although the jury is still out, Aum may have been unique. Even the Minnesota Patriots Council, which developed ricin because they believed it to be used by the CIA and the KGB, never conceived of using it in the same manner as the Bulgarian secret service. Rather than use an umbrella, the MPC experimented with using hand lotion as a means of dissemination.

For another, an umbrella (even one involving a chemical or biological weapon) simply does not offer the same level of destruction, the same "bang for the buck" as other terrorist methods. Not even the Weather Underground, whose name would seem to imply an interest in such methods, showed evidence of ever considering using umbrellas in any of their attacks. Instead, they chose the symbolic bombing of the imperialist power structure. So the answer is yes, the standard terrorist arsenal is now the gun, the bomb, the plane bomb, box cutters, and even the umbrella or anything else they can get their hands on. As all of us witnessed on 9-11, Osama bin Laden did try such a method of attack, and it brought a whole new meaning to his "umbrella terrorist network."

HACKER-CONTROLLED TANKS, PLANES, AND WARSHIPS

Army officials are worried that sophisticated hackers and other cyber criminals, including military adversaries, may soon have the ability to hack their way into and take control of major military weapon systems such as tanks and ships. The potential exists for hackers to infiltrate the computer systems used in tanks and other armored vehicles. Unlike in the past, today's modern tanks and ships are almost entirely dependent on computers, software, and data communications links for functions such as navigation, targeting, and command and control.

Although the Pentagon has had computer security issues to deal with for a long time, they've never had computers in tanks and armored personnel carriers before. In fact, the Defense Department (DoD) has already tested and proven that hackers

→

have the ability to infiltrate the command and control systems of major weapons, including Navy warships. According to a training CD-ROM on information assurance, published by the Defense Information Systems Agency, an Air Force officer sitting in a hotel room in Boston used a laptop computer to hack into a Navy ship at sea and implant false navigation data into the ship's steering system.

Yes, this actually happened. The CD-ROM instructs military personnel taking the course. Fortunately, this was only a controlled test to see what could be done. In reality, the type of crime and its objective is limited only by people's imagination and ability.

Although there are well-known security gaps in the commercial systems that the Army plans to use on the battlefield, hacking into tanks and other weapons may be too difficult for an enemy engaged in battle. The problem for the enemy is that computer security vulnerabilities will almost certainly prove fleeting and unpredictable. Such tactics would be nearly impossible to employ beyond the random harassment level.

It is imperative for the United States to study what it means to be a superpower in the Information Age. In addition to the two dozen countries known to be pursuing technologies that would enable them to produce weapons of mass destruction, threats to the nation's critical infrastructure from cyberattacks are also high on the present administration's list of things to prepare for.

Other countries are forming cells of professionals dedicated to finding ways to interrupt the United States' information infrastructure. If you can shut down the United States' financial system, if you could shut down the transportation system, if you could cause the collapse of an energy production and distribution system just by typing on a computer and causing those links to this globalization to break down, then you're able to wage successful warfare, and the United States has to be able to defend against that. The United States is presently taking on those defense measures.

U.S. Government Agencies Shape Cyberwarning Strategy Against Terrorists and Rogues

Under pressure from Congress to better coordinate the government's response to computer viruses and other cyberattacks by terrorists and rogue states, the National Security Council (NSC) has developed a plan outlining roles and responsibilities for federal cybersecurity organizations. Under the plan, the National Infrastructure Protection Center (NIPC), working with the General Services Administration's Federal Computer Incident Response Capability Office, will take the lead in alerting agencies to cyberattacks and will coordinate any immediate response.

The memo describing this plan identifies the organizations and agencies to be involved in various kinds of attacks and defines the criteria for NIPC to call a meeting of the full cybersecurity community. According to the plan The NSC will step in whenever a security response requires a broad policy decision. This institutionalizes how the United States will share information, both at an operations level and at a policy level when cyberincidents occur. Many observers have called for coordination among organizations such as NIPC, the Critical Infrastructure Assurance Office (CIAO), and NSC.

NIPC, based at the FBI, was established in 1998 to serve as the government's central organization to assess cyberthreats, issue warnings, and coordinate responses. The CIAO was set up to help agencies develop and coordinate security policies and plans. The proliferation of organizations with overlapping oversight and assistance responsibilities is a source of potential confusion among agency personnel and may be an inefficient use of scarce technical resources. The calls for coordination became louder after the "I Love You" virus affected almost every federal email server and taxed many agencies' resources. The lack of formal coordination and communication led to many more agencies being affected by the incident than necessary, according to the Government Accounting Office.

Although the many warning and response organizations work together, the NSC memo lays out a standard process for coordination. In the past, that type of coordination happened on an ad hoc basis. Now, as laid out in the memo, the process is set so that it can last into the next administration in 2005 and possibly to 2009.

Some of the formal mechanisms that existed were frankly ineffective in the tasks they were meant to do. For circumstances that are extraordinary, the United States now has a process by which the NIPC will coordinate the operational response, and the NSC will head the policy response.

THE DARK WORLD OF THE CYBER UNDERGROUND

It was nearly Christmas (1998) when Dionne Smith received an alarming letter that dampened her holiday spirit—to say the least. The anonymous note warned Smith, 31, an employee of a Los Angeles parking company, that by opening the envelope she had just exposed herself to the biotoxin anthrax, a livestock bacteria that can be fatal if inhaled. The 1998 Christmas incident was a horrible and frightening experience—which was one of approximately 220 nuclear, biological (see sidebar, "Bioterrorists on the Green"), and chemical scares (including some 140 anthrax false alarms) in this country alone.

BIOTERRORISTS ON THE GREEN

Will the next terrorist attack be against plants, not people? At the urging of the White House, the U.S. Department of Agriculture and the FBI are looking at the

→

threat of agricultural bioterrorism—an assault on the country's efficient but fragile system of giant single-crop farms. The fear is that if some party wanted to, they could damage a major crop—and the economy—by introducing a plant pathogen that doesn't normally exist here. Likely bioweapons include plant-killing fungi, such as soybean rust, or infectious microbes that induce plants to produce toxins. If the group were sophisticated enough, they could genetically engineer a highly pathogenic strain, produce it in large quantities, and sneak a lot of it in.

In wild plants, natural genetic diversity helps limit the spread of disease. Ninety-nine percent or more of the genes in crops are the same across the United States, and that uniformity makes an epidemic much more likely. Once unleashed here, a superbug could spread like wildfire before researchers identified it and figured out how to keep it in check. Even then, spores could survive and infect the next year's crop. They could also be spread by the wind, from field to field, or even state to state. It would be a continuing, recurring problem, like a permanent bomb going off.

Even though so far they've all been fakes, the feds are on edge. Their major worry is that terrorists are adding chemical and biological weapons to their arsenal of arms, and that, one day, they'll make good on their threats. So the government has begun taking precautions and has poured billions of dollars into creating a network of programs designed to respond to such attacks. The ambitious plans include amassing antidotes to potential bioagents such as anthrax and other bacteria and viruses and to chemical weapons such as the nerve agent sarin. The government is training medical response, fire, police, and rescue teams; beefing up local health departments to care for civilians in case of a major attack; and gathering intelligence on terrorist groups believed to be interested in acquiring such weapons. These new programs have helped make counterterrorism one of the fastest-growing parts of the federal budget, even as terrorist acts plunged to a 33-year low prior to the 9-11 attacks, according to congressional budget analysts. Total U.S. antiterrorism spending could exceed $90 billion in 2005, up from $60 billion in 2002. The question is whether it's money well spent.

A recent report by the General Accounting Office, Congress's watchdog, says no, claiming that lawmakers have dumped money into fighting a threat yet to be fully assessed and probably less dangerous than widely believed, considering how tough it is to acquire, process, and use the deadly toxins. A growing number of government and private counterterrorism experts agree. They say that federal officials are so spooked by the possibility of a chemical or biological attack that they are deliberately hyping the threat to get Congress to cough up coveted cash for prevention programs, and most lawmakers are buying it wholesale. It's Mom, apple pie, and terrorism. In 1997, a jittery Congress ordered the DoD to conduct multiagency training exercises in the nation's 120 largest cities against so-called weapons of mass destruction. Today, there are some 400 training courses run by myriad agencies, including the Energy and Justice Departments, the Environmental Protection Agency, and the Federal Emergency Management Agency (FEMA). In just how many different ways is the United States going to set out to accomplish the same thing, because many of the programs are redundant?

The most eye-popping example of out-of-control spending, detractors say, is the Department of Health and Human Services (HHS). In 1996, HHS spent $7 million on its "bioterrorism" initiative. In 2004, it requested $785 million. Most notably, the department intends to create a national stockpile of millions of doses of vaccines and antibiotics, a potential boon for pharmaceutical companies that are among those eagerly lobbying for more antiterrorism measures. Government Accounting Office investigators have repeatedly questioned the department's emphasis on vaccines for smallpox, pneumonic plague (airborne bacteria that cause respiratory failure), and tularemia (bacteria that cause a disabling fever in humans). None of these potential killers appear on the CIA's list of biggest germ threats from terrorist groups. Still, HHS is doing the right thing by focusing on them. Tularemia and pneumonic plague are very easy to develop. The easiest to develop is anthrax.

Other agencies are clamoring for a piece of the pie, leading to tremendous internecine fighting. FEMA wants a chunk of the training and equipment money, as does the Justice Department's Office of Justice Programs, whose mission is to dole out federal anticrime money to states and localities. The Department of Veterans Affairs wants to wrest stockpiling duties away from the Centers for Disease Control and Prevention, and the National Guard, a powerful lobby on Capitol Hill, is creating its own hazardous materials response teams, even though there are already more than 800 state and local hazardous material (HAZMAT) units, plus additional crews in the Army, Marine Corps, EPA, and Coast Guard. Then there's the Energy Department, which is pushing for $80 million to research palm-size bug and poison detectors and other antiterrorism products. Not to be left out, the United States Holocaust Memorial Museum and the Office of Personnel Management want $6 million apiece, and the Smithsonian Institution is asking for $7 million to bolster security against potential terrorist attacks.

When Congress first began considering this issue in 1995, the debate was driven by the belief that terrorists, although more likely to use guns and bombs, would eventually turn to lethal chemical and biological agents. The 1995 Tokyo subway gas attack by the cult Aum Shinrikyo was a shot across the bow. So were reports that Osama bin Laden—accused of masterminding the bombings of two U.S. embassies in East Africa—had tried to get his hands on unconventional weapons.

The only major case of bioterrorism in the United States was in 1984 by followers of the Indian guru Bhagwan Shree Rajneesh, who had set up a commune in Oregon. Hoping to sway a local election, they unleashed salmonella poisoning in 10 restaurants in a nearby town, sickening 751 people but killing none. Still, law enforcement officials are convinced that the risk merits whatever preventive measures the government can afford. This is not on the top 100 list of things you're going to die from, but if you're a national security expert, this is on the top 3 list of things to worry about.

One reason there have been no attacks is that it's so tough to effectively use biological weapons, but a dozen hostile nations now either possess or are actively pursuing bioweapons. Most counterterrorism and intelligence experts agree that other countries would think hard before striking, because they know the United States would retaliate with stunning force. They also agree that terrorists cannot carry out large-scale lethal attacks without the backing of a foreign government. However, they can do damage. The question is, how much? Nobody knows, because few have bothered to assess how real the threats are. No one, though, wants to be caught asleep at the switch—just in case. It's one of those things it's hard to say no to. It's like fallout shelters in the 1950s. Was that wrong to do? You have to look at the world you're operating in.

THE CRIMINAL CAFÉ IN CYBERSPACE

Not long ago, if a terrorist wanted to cause a blackout in, say, New York, it would have taken some work. He or she might have packed a truck with explosives and sent it careening into a power plant. Or he or she might have sought a job as a utility worker to sabotage the electrical system. Now, intelligence experts say, it's possible for a trained computer hacker to darken Gotham from the comfort of home or a cybercafé (at a coffee house). Worse, his other home might be as far away as Tehran, Iran. Worse yet, he or she may enjoy the full backing and technical support of a foreign government.

In a closed briefing to Congress, the CIA reported that at least a dozen countries, some hostile to America, are developing programs to attack other nations' information and computer systems. China, Cuba, Russia, Korea, and Iran are among those deemed a threat, sources later declared. Reflecting official thinking no doubt, the *People's Liberation Daily* in China noted that a foe of the United States only has to mess up the computer systems of its banks by high-tech means. This would disrupt and destroy the U.S. economy. Although the specifics are classified, a new National Intelligence Estimate reports at least one instance to date of active cyber-targeting of the United States by a foreign nation.

Officials are worried because so much of America's infrastructure is either driven or connected by computers. Computers run financial networks, regulate the flow of oil and gas through pipelines, control water reservoirs and sewage treatment plants, power air traffic control systems, and sustain telecommunications networks, emergency services, and power grids. All are vulnerable. An adversary capable of implanting the right virus or accessing the right terminal can cause massive damage.

In 1996, a Swedish hacker wormed his way through cyberspace from London to Atlanta to Florida, where he rerouted and tied up telephone lines to 11 counties, put 911 emergency service systems out of commission, and impeded the emergency responses of police, fire, and ambulance services. There have been many domestic cyberattacks as well. The number of pending FBI cases involving computer crimes (a category that includes computer infrastructure attacks and financial crimes) increased from 451 in 1999 to about 1,100 in 2004.

In 1997, intelligence officials got a glimpse of what's possible during an information warfare exercise named "Eligible Receiver." The secret war game began with a set of written scenarios in which energy and telecommunications utilities were disrupted by computer attacks. In one scenario, the attackers targeted the 911 emergency phone system by telling Internet users there was a problem with the system. The scenario posited that people, driven by curiosity, would phone 911 and overwhelm the system.

"Eligible Receiver" culminated when three two-person "red teams" from the National Security Agency used hacker techniques that can be learned on the Internet to penetrate DoD computers. After gaining access to the military's electronic message systems, the teams were poised to intercept, delete, and modify all messages on the networks. Ultimately, the hackers achieved access to the DoD's classified network (see sidebar, "Espionage By Keystroke?") and, if they had wished, could have denied the Pentagon the ability to deploy forces. In another exercise, the DoD found that 74% of test attacks on its own systems went undetected.

ESPIONAGE BY KEYSTROKE?

Forget about signal sites and dead drops (like the recent FBI Russian mole case of suspected spy Robert Phillip Hanssen). The classic tropes of the spy game have gone the way of the Model T. When an FBI computer jock finally hacked his way into Aldrich Ames's personal computer a few years ago, investigators were dumbfounded by the number of secrets he'd purloined from the CIA—hundreds of stolen documents and classified reports. FBI brass called Ames the worst case of treason in U.S. history.

The preceding could be peanuts compared to the Wen Ho Lee case. Government officials confirmed that scientist Wen Ho Lee, suspected of stealing classified data from a secret weapons laboratory, downloaded reams of classified nuclear weapons information from a high-security computer system to one that could be accessed with relative ease.

→

> Actually, reams doesn't begin to describe the dimensions of it. The FBI is talking about millions of lines of computer code here, data bits gathered during the course of 53 years of research and more than 5,000 nuclear tests—information that shows how the nation's most sophisticated nuclear weapons work. With a few simple computer strokes, in other words, someone made America's national-security crown jewels available to any reasonably sophisticated person in possession of a computer, a modem, and the file names under which the information was stored. It is flabbergasting. There's just no other word for it.
>
> The someone in question was Wen Ho Lee, a Taiwan-born scientist employed, until recently, at the Department of Energy's weapons laboratory in Los Alamos, New Mexico. Lee was dismissed from his job in 1999 for security breaches after it was disclosed that he was the subject of an FBI espionage investigation. Prosecutors have not charged Lee with spying, and he has asserted his innocence, but when FBI agents searched Lee's computer after his dismissal, officials say, they discovered that he had transferred an incredibly large amount of nuclear data from the Energy Department's high-security computers to the more accessible network, dumped the information under bogus file names, then tried to erase the evidence from his hard drive. The transfers occurred between 1983 and 1995, but accelerated in 1994 and 1995, when Los Alamos began installing a new system designed to impede such transfers.
>
> The evidence gathered to date does not show that the security breach resulted in damage on a massive scale, but it is huge nonetheless. The FBI is still investigating whether anyone accessed the data from the low-security network to which Lee transferred the information. Some officials say that may never be known for sure.
>
> Like every espionage investigation, the Lee case is rife with peculiarities. Lee first came under suspicion in 1996, after the CIA obtained a document showing that China's military had obtained classified information about the size and shape of America's newest miniaturized nuclear warhead, the W-88. The FBI was slow to investigate Lee, in part because Lee's wife was working as a confidential informant for the bureau, but there were other problems. When agents in the FBI's Albuquerque field office pressed for a search warrant in Washington, lawyers at the Justice Department rebuffed the request. The Foreign Intelligence Surveillance Court has almost never rejected a search warrant request, and bureau officials indicate this rejection was unwarranted. In any case, by that time the damage was done.

In 1998, the FBI raided the homes of two California high school sophomores. Their hacker assaults on the Pentagon, NASA (which was very easy), and a U.S. nuclear weapons research lab were described as the most organized and systematic attack on U.S. computers ever discovered. To make the Pentagon attack hard to trace, the hackers routed it through the United Arab Emirates. They were directed by a teenage hacker in Israel.

To help industries fend off hacker attacks, both foreign and domestic, the government has created the National Infrastructure Protection Center, to be staffed by 458 people from the FBI, other agencies, and industry. Recent events make clear that tighter defenses are needed. In 1997, a 13-year-old boy with a home computer disabled control-tower communications at a Worcester, Massachusetts, airport for nine hours. The loopholes the teenager exploited have been closed, but no computer environment is totally secure. Preventing hacker attacks is like a never-ending journey. You will never get to your destination.

Chinese Cyber Criminal Café Hacktivists Spin a Web of Trouble at Home

In the university district of Beijing, a bunch of 20-year-olds calling themselves the "Web Worms" slouch around in an apartment stacked with old issues of *PC* magazine. Chinese computer networks are easy to break into. Ninety percent of them are not secure.

From the moment in 1995 that a commercial Internet provider first gave Chinese citizens access to the Web, the government has tried to maintain what some cybersurfers derisively call "the Great Firewall of China." This elaborate control system is supposed to block sites that the Communist Party considers morally or politically degenerate, from Penthouse to Amnesty International to CNN, but with a few simple tricks, ordinary Internet users are now making a mockery of the Great Firewall, tapping easily into forbidden foreign sites.

Sabotage

Sophisticated hackers, meanwhile, are breaking into sensitive Chinese computers (see sidebar, "Cyberspace Incidents on the Rise in China"). Members of the Hong Kong Blondes, a covert group, claim to have gotten into Chinese military computers and to have temporarily shut down a communications satellite last year in a "hacktivist" protest. The ultimate aim is to use hacktivism to ameliorate human rights conditions.

CYBERSPACE INCIDENTS ON THE RISE IN CHINA

Intelligence and security experts are warning foreign firms in China of a growing threat of Internet-related crimes, government surveillance, and loss of proprietary data, but some U.S. companies said they view those threats as exaggerated. The latest warning comes from a report published in 2004 by a network security firm founded by two former U.S. Navy intelligence officers. The report cautions companies that the

→

government-controlled Internet environment in China could put the integrity of their networks at risk.

The most important consideration is that, in one way or another, the government is involved in the operation, regulation, and monitoring of China's networks. As a result of this and other factors, such as tensions with Taiwan, U.S. companies could see an increase in scans, probes, and attacks that could be aimed at gaining technical information.

Representatives from companies with major operations in China indicate that they have never had problems and don't plan to run scared now. The companies discount most of the alarmist reports. The real focus of the control efforts is what the Chinese call "black and yellow," or political and pornographic, material. How serious an issue economic espionage is depends on who you are and what business you're in, and economic espionage isn't unique to China.

Nevertheless, other companies are not convinced that the Chinese government is overtly (or, for that matter, covertly) engaging in corporate espionage via the Internet. Yet U.S. intelligence experts warn that China's vast intelligence-collecting apparatus has a voracious appetite for any U.S. technology that could help speed the People's Republic's military modernization and boost the country's economy. That puts high-tech vendor companies particularly at risk.

Businesses operating in China are up against a national government that has essentially unlimited resources and a long track record of industrial and economic espionage. Every business in China is run by the government; any effort to develop intelligence and promote those industries is a national effort. Scans, probes, and attacks against U.S. firms in China are statistically confirmed and growing and could be Chinese tests of offensive IW tactics or the work of Chinese virus writers.

The U.S. firms that may be at the greatest risk of losing proprietary data include companies that have set up development laboratories in China, but those companies, eager to gain a foothold in China's burgeoning information technology (IT) market, don't necessarily share the fears of intelligence experts.

Nonetheless, there are more controls in place in China than in some other countries, but they have not been put in place to foster espionage. Although the Chinese view controls and regulations as necessary to facilitate an orderly Internet market and to protect the country from subversion and other Internet crimes, the controls are partially the result of political rigidity and bureaucratic inertia. Human nature is the same everywhere in the world. The thought that there are lots of people with time on their hands to explore what the 50 million Internet users in China are doing is totally impractical.

Free speech also is proliferating in China. A political journal called *Tunnel* (*http://www.geocities.com/SiliconValley/Bay/5598/*) is said to be edited secretly in China and sent by email each week to an address in the United States, from which it is then emailed anonymously back to thousands of Chinese readers. *Big Reference* (*http://www.ifcss.org/home/*) is another online challenge to the authorities. One recent issue extolled individualism and paid tribute to the mother of a student killed when troops crushed the pro-democracy protest in Tiananmen Square in 1989.

The Internet provides not only speed and efficiency but also cover. If you tried to publish a traditional newsletter promoting democracy in China, you'd surely get arrested. If only the authorities were smart enough to realize what's going on, all the political activities on the Internet would really have them scared.

Perhaps they are smart enough. Regulations introduced in 1997 imposed stiff penalties (including jail sentences) for using the Internet to damage state interests, spread rumors, or publicly insult others. Nonetheless, China's wired population has grown to 7.731 million according to government figures. Although that is a tiny portion of an overall population approaching 4 billion, China's Internet users are virtually by definition the country's most educated and modern elite. To watch over them, a new force of more than 500 "Internet security guards" has been assigned to patrol computer networks at state companies and ministries. What the Chinese government is really afraid of is political infiltration. The government's goal is to have a security guard in every work unit.

Perhaps most worrisome to the authorities, young Chinese are using the Net to coordinate political campaigns. On August 17, 1998, Indonesia's independence day, hackers in China broke into Indonesian government Web sites and posted messages protesting violence against ethnic Chinese there. Chinese security officials ignored the demonstration until it reached the streets. That day, about 200 students rallied outside the Indonesian Embassy, carrying photographs of rape and murder victims that they had downloaded from the Web. The incidents weren't written up in the Chinese news, but were posted on the Web.

Recently, the government has taken even more drastic action. In Shanghai, a computer engineer named Lin Hai faces charges of inciting the overthrow of state power by providing 60,000 email addresses to *Big Reference*. And at the end of 2000, the publishers of *Tunnel* went into hiding.

THE SUPER COMPUTER LITERATE TERRORIST

During the next 20 years, the United States will face a new breed of Internet-enabled terrorists, super computer literate criminals, and nation-state adversaries who will launch attacks not with planes and tanks, but with computer viruses and logic bombs. America's adversaries around the world are hard at work developing tools to bring down the United States' private sector infrastructure. The United States faces an increasingly wired but dangerous world, as evidenced by the following:

- Many countries have programs to develop cyberattack technologies and could develop such capabilities over the next decade and beyond.
- The Unites States, Russia, China, France, and Israel are developing cyberarsenals and the means to wage all-out cyberwarfare.
- Terrorist groups are developing weapons of mass destruction.
- Russia has become a breeding ground for computer hackers. The Russian equivalent of the U.S. National Security Agency and organized crime groups recruit the best talent.
- Electronic stock scams, robberies, and extortions are proliferating.

A report by the Washington-based Center for Strategic and International Studies (CSIS) went even further, warning of a future cyberarms race and the rise of terrorist groups supported by super computer literate youngsters bent on disrupting the Internet. China is of particular concern here, because it's devising strategies for unrestricted electronic warfare. Officials say critical infrastructures in the United States could be targeted in the future as revenge for incidents like the 1999 accidental bombing of the Chinese embassy in Serbia. The Chinese government has even suggested having every person in China send one email to an address of interest in the United States or use hacker tools easily available on the Internet to support a mass denial-of-service attack.

Online extortion and falsification of shipping manifests by criminals and attempts by countries to use hacking techniques to evade trade sanctions are a rising concern. DoD officials are also becoming increasingly concerned about the proliferation of "always-on" Internet appliances such as modems and network printers. Hackers are finding ways to penetrate these devices and possibly use them as launching pads for more devastating distributed denial-of-service attacks. For example, in 2000, a hacker cracked into a printer at the Navy's Space and Naval Warfare Center and rerouted a potentially sensitive document to a server in Russia.

Therefore, the real threat comes from the design of the U.S. infrastructure and the people who run it. Companies build these systems and their business models on the assumption that things will always work. If a major attack is made on the infrastructure, it's going to happen from the inside.

The aforementioned reports hold a powerful message for the national cybersecurity effort. However, that future preparedness will be determined by how much emphasis companies and the government place on fixing known vulnerabilities, training and education, and enforcing good security policies.

Although the threat of terrorists groups attacking the infrastructure is real, a word of caution is needed. It's scary, but it's really hard to bring down the Internet.

THE NEW SECURITY PROFESSIONALS

At a table equipped with two computers, Mark Coletta (not his real name to protect his privacy) plies his trade. The intense, lanky 27-year-old is hunting for holes in a corporate network. Mark seeks clues that will reveal operating systems, firewalls, or user names. Any one of these could become a key for breaking into the system. He thinks purely as a brilliant but nasty rogue hacker, but Mark is no malicious rogue hacker. He's a security engineer at an information security company where he's paid to tinker with clients' networks and uncover their vulnerabilities.

With cyber crime increasingly making news headlines, services such as vulnerability assessments, integration of firewalls and other security components, and subscription-based managed security are in high demand. That demand is spawning a lucrative market. IT security services will generate up to $13.1 billion worldwide in 2006 and are growing at a per-year compound rate of 54%, according to predictions of the research firm GartnerGroup.

Most other security people are vulnerability experts who have switched their black rogue hacker hats for white hats. Many ex-hackers have become security consultants. Their vision now is to simplify the security process, using the Internet by documenting the best security practices and then providing them to clients over the Web. Tying security into a company's e-commerce [3] strategy also is key. Most people in this business are just out of school.

Meetings with prospective clients begin with a knowledge test of what and whom the security specialist knows. Once some sort of connection is established, the client will pose technical questions about any number of areas, such as databases, Unix, or the Novell platform. What makes the security professional different from other IT professionals is that they have to know something about everything. Some clients, influenced by media reports of computer crimes or by upper management pushing a security plan, are ready to "pull the trigger" immediately. Others, though, are hit with sticker shock. They don't understand how much security costs. Mark has to provide a clear return on investment statement. It's the same problem an insurance agent has. Mark has to identify the probability that something will happen—it's the downstream effect.

To devise a security plan for a client, Mark makes a technical assessment of a network and combines it with his own interviews and observations. He assesses a company's "pain threshold," or how much security risk it can endure before the business would shut down. Once completed, a security plan can be 700 pages long. Mark then either implements the plan or recommends how the client can enact it.

THE MIDDLE EAST CYBERWAR

Palestinian supporters use a combination of hacking tools and viruses to gain what appears to be the upper hand in the Middle East's ongoing cyberwar. How Palestinian hackers watch and what they know will determine the success of this cyberwar for them.

They distribute the tools and viruses for destroying Israeli sites using a recently created attack site. Visitors to the site are greeted with the message, "I swear that I will not use these programs on anyone but Jews and Israelis." The site comes complete with a list of directions on how to use the attack tools. LoveLetter, Chernobyl (CIH), and the Melissa Virus (along with 12 Word macro viruses) form the arsenal for attacking Israeli sites. Apparently, it's an effective system.

According to sources at iDefense, an international security firm monitoring the situation, pro-Palestinian hackers use a variety of tools to orchestrate a well-organized attack against the 400 or more Israeli Web sites that have been hit during the conflict. It is hard to say for sure who is winning, but it appears that the pro-Palestinian hackers have successfully affected more sites. The pro-Palestinians have been much more aggressive in scope. Instead of just targeting specific sites, they have methodically worked through all the sites, thus broadening their agenda.

Over 559 Web sites have been targeted by both sides for denial-of-service attacks, attempts to gain root access, system penetrations, defacements, and a variety of other attacks. Many sites have been indirectly affected because of the strain that the attacks have placed on the Net infrastructure in the Middle East.

The conflict began on October 6, 2000, when pro-Israeli hackers created a Web site to host FloodNet attacks. Since then, both sides have sustained blows to vital information and financial-resource sites such as the Palestinian National Authority site and the Tel Aviv Stock Exchange. Sixteen tools have been identified as those actively distributed among attackers, with many others being discussed or suspected of already being deployed. One such tool is called the EvilPing, believed to have been created especially for this war. The tool launches a "ping of death attack" that, when utilized by several users against the same target, crashes the system.

Then there is QuickFire, an attack tool that sends 32,000 emails to the victim from what appears as the same address. Used simultaneously by multiple attackers, the tool crashes an email server. *QuickFire* strength is that it does not relent, continually firing off thousands of emails until the server is shut down and the address blocked. It is believed to be the tool used for hack attacks on the Israeli Foreign Ministry site and its Webmaster's email address.

A group called Hackers of Israel Unite originally used another popular tool called WinSmurf, which also uses mass pinging to bring down a site. Borrowing amplifying power from broadcast sites, the hackers send out pings that are boosted 10,000-fold or more. According to the group, they were able to shut down Almanar.org using one computer with a 56K modem and an ADSL line.

According to Netscan.org, a site that provides a list of broadcast sites with an average amplification of times five, a dial-up user with 28.8 kbps of bandwidth, using a combination of broadcast sites with an amplification of 40, could generate 1152.0 kbps of traffic, about two-thirds of a T1 link. With tools like these, a 56K can become a powerful weapon and your bandwidth is irrelevant. Netscan.org creators call themselves a small group of concerned network administrators who got fed up with being smurfed all day, but they recognize that their site has also become a hacking tool.

Pro-Palestinians recently turned the tables by using broadcast-site attack tools against Israeli sites. Although the leaders in the war (groups such as UNITY, DoDi, and G-Force Pakistan) remain in the limelight, many previously unknown hackers are taking the cyberwar to another level. Hackers are making moves to gain root access to Israeli computers and servers. Root access is the ultimate possession; it means doing whatever you want with a system. In essence, a hacker who gains root access control of a computer can scan, delete, and add files, use it as an attack tool against others, and even view and hear users whose computers are equipped with cameras and microphones.

With no end in sight to the Middle East cyberwar, talk of targeting U.S. interests on the Web has been popping up in chat rooms and Internet Relay Chat (IRC) channels frequented by pro-Palestinian hackers. Hackers such as DoDi have come out and said that the current war isn't just against Israeli, but the United States as well. Arab activists such as Mustapha Merza believe the American media continues to portray Arabs as terrorist aggressors, even in cyberspace.

The irony is that the number of times that U.S. government sites have been targeted by Israelis are more numerous than those times they were targeted by pro-Palestinians, yet the American media fails to identify the real perpetrators and victimizes the Arabs as usual. For its part, the National Infrastructure Protection Center (a division of the FBI concerned with cyberwarfare, threat assessment, warning, and investigation) lists both Israeli and Arab sites that promote the cyberwar.

How Israelis Watch and What They Know

A group of self-described ethical hackers are taking the reins of Israel's Web networks into their own hands in the Middle East's cyberwar. Known as the Israeli Internet Underground (IIU), the coalition of anonymous online activists from various Israeli technology companies has set up a Web site to disseminate information concerning the ongoing battle in cyberspace.

According to the IIU mantra, they are dedicated to the Israeli spirit and united to protect Israel on the Internet against any kind of attacks from malicious hacking groups. The site claims to provide a comprehensive list of sites that were hacked by Arab attackers since the cyberwar went into full swing in October 2000. Listed are over 80 Israeli sites that have been defaced and vandalized by various hacking groups. The number coincides with estimates provided by officials at iDefense. IIU also provides a list of Israeli sites that they believe run services with commonly known security holes such as BIND NXT overflow, IIS 4 holes, and FTP format string bugs.

Examples of defacements by Arab hackers such as the one perpetrated on the homepage of Jerusalembooks.com, one of the largest Jewish booksellers on the Web, serve as a warning to those Israeli sites with suspect security. The Jerusalembooks.com text and graphics were recently replaced with the word "Palestine" in flaming letters and with text asking Israelis if the torah teaches them to kill innocent kids and rape women. The site is currently under reconstruction because of the attack.

Taking credit for the attack is the group GForce Pakistan, a well-known activist group that has joined forces with Palestinians and other Arab hackers in fighting the cyberwar against Israeli interests. Working alongside the group is the highly skilled Arab hacker named DoDi. On November 3, 2000, DoDi defaced an Israeli site and stated he could shut down the Israeli ISP NetVision, host of almost 80% of the country's Internet traffic.

Though petty defacements and racial slurs have been the norm on both sides of the battle, Arab hackers like DoDi have promised to kick the war into high gear in the coming years, implementing what they refer to as phases three and four of their "cyber-jihad."

The Muslim extremist group UNITY, with ties to Hezbollah, laid out a four-part plan for destroying the Israeli Internet infrastructure at the onset of the cyberwar. Phase four culminates in blitzing attacks on e-commerce sites, causing millions of dollars of losses in transactions. IIU said there is already evidence of phase-four attacks, such as the destruction of business sites with e-commerce capabilities, which they believe caused a recent 12% dip in the Israeli stock exchange.

The current onslaught of cyberattacks against Israel's key Web sites is perhaps the most extensive, coordinated, and malicious hacking effort in history. ISPs and e-businesses must recognize the need to install protection that goes beyond firewalls to provide real security against application-level assaults.

In order to thwart future attacks, IIU has created what they call the SODA Project (sod is Hebrew for secret). The stated goal of the project is to inform and provide solutions wherever the IIU can and, therefore, protect their sites against political cybervandalism. It lists those Web sites with security vulnerabilities, making them susceptible to future attacks by Islamic groups.

The SODA Project formed an alliance with the Internet security firm 2XS Ltd., which is linked to the site and agreed to provide security advice for casualties of the cyberwar. 2XS Ltd., however, does not accept responsibility for IIU actions. On November 3, 2000, IIU contacted 2XS Ltd. to share their idea of creating a site for publishing vulnerability alerts. Another link on the SODA Project is the Internet security information forum SecurityFocus.com, a resource guide to online security links and services based in San Mateo, California. The site is not taking any sides in the Middle Eastern war.

Typically, the odds are heavily in the attackers' favor—the attacker can launch attacks against any number of sites at little to no cost. They only need to find one vulnerable victim to succeed, perhaps after checking thousands of potential victims.

Because both Arabs and Israelis are launching volley after volley against the others' sites, neither faction gets to play the victim in this war. The victims end up being citizens and businesses in the affected area. Unfortunately, that's not uncommon in that part of the world.

THE NEW TOOLS OF TERRORISM

Despite increasing concern about cyberterrorism, the tactics and goals of the world's terrorist organizations remain low-tech. Although the terrorist's toolbox has changed with the advent of the Information Age, the objectives of the world's terrorist organizations have not. A growing percentage of terrorist attacks are designed to kill as many people as possible. Guns and conventional explosives have so far remained the weapons of choice for most terrorists.

However, terrorists are adopting information technology as an indispensable command-and-control tool. Raids on terrorist hideouts, for example, are increasingly likely to result in the seizure of computers and other IT equipment. Instead of just finding a few handwritten notebooks and address books, counterterrorism authorities are faced with dozens of CD-ROMs and hard drives. Likewise, terrorists' increasing use of advanced encryption tools often delays the process of finding key files and information.

Terrorists groups, such as the Osama bin Laden organization, have yet to demonstrate that they value the relatively bloodless outcome of a cyberattack on a nation's critical infrastructure, but the threat remains real. The warning signals are out there. If the United States fails to recognize this, then the United States will pay another high price like they did on 9-11.

Information Weapons

There are several weapons or tools currently available that can negate, destroy, or incapacitate information systems, with many more being rapidly developed. In this section, these are broadly grouped into three main types: high energy radio frequency (HERF) guns, electromagnetic pulse (EMP), and other information weapons.

HERF Guns

A HERF gun (as discussed briefly in Chapter 13) is a device that directs high-power radio energy at an electronic target. Electronic circuits are vulnerable to overload; a HERF gun simply overloads particular circuits to disable specific pieces of equipment that are dependent on that circuit. A HERF gun can be designed to cause varying degrees of damage from shutting a system down to physically destroying equipment. Pointed at a computer, a HERF gun may either permanently or temporarily terminate its operations. A HERF gun pointed at a "fly-by-wire" aircraft may trigger a catastrophic failure.

Although currently limited in range and destructive capacity, in the near future, HERF guns are likely to be substantially more capable and freely available and, therefore, must be taken seriously. HERF guns represent an excellent addition to the offensive military inventory of a nation and a significant threat if possessed by an enemy. The defensive measures that can be employed to reduce the risks of HERF attacks are not well developed at this stage but include using Gaussian shielding, gaseous discharge devices, and the maintenance of physical separation.

Electromagnetic Pulse

EMP has been described as the next great weapon to evolve in modern warfare. Initially discovered as a side effect of nuclear tests, the phenomenon has now been extended to nonnuclear generators. Such generators can create an EMP that will disable unshielded electronic systems. A development beam generator with a 1 gigawatt capacity could be used to develop a line-of-sight EMP that would knock out most unshielded electronic devices within a radius measurable in tens to hundreds of meters, depending on the employment method. High-power microwaves and communications, computer, navigation, and data processing systems would be most affected by such weapons. The current limitations of these weapons are power generation and capacitor storage capability, but these can be expected to be overcome in the future.

Research is well advanced, with EMP warheads recently being fitted on U.S. Air Force air-launched cruise missiles. EMP weapons are less discriminatory than HERF guns and could be used to shut down a general area rather than a specific system. Again, with the exception of screening techniques such as Gaussian shielding, defensive measures are not common.

Other Information Weapons

Several weapons are currently being developed that do not fit in the HERF or EMP categories. Some already are in service with various military forces; others remain on the drawing board. The following weapons are described in a variety of freely available publications and give an indication of the technologies being developed and the possible capabilities that may result.

Low-Energy Lasers

These lasers can be used to damage the optical systems of sensors (including data collection devices), thus attacking the information systems at the data collection level. Low-energy lasers have already been fitted on rifles and armored vehicles and were deployed during the Gulf War. A number of systems are reported to be under further development in the United States and United Kingdom.

Electric-Power Disruption Technologies

An electric-power disruption weapon was first used during the Gulf War in 1991. The technology originated after an accident on the U.S. West Coast when chaff cut power supplies to the city of San Diego in 1985. The weapon uses light conductive carbon fibers that wrap around transmission lines and distribution points to cause a massive short circuit. Even when power is restored, the fibers must be removed because any breeze can result in another short circuit. This weapon can be delivered by cruise missiles, as was the case in the Gulf War, or from manned aircraft.

Individually, each of the military information operations (MIO) tools (discussed in Chapter 13) and techniques just described will present a military commander, whether operating in the conventional or IW environment, with a substantial force multiplier. Collectively, they offer a decisive addition to military power. As more MIO capabilities are developed, the effectiveness of the MIO strategy will increase exponentially, reflecting the synergistic relationship that exists between individual elements of the MIO environment. Accordingly, nations developing information strategies should consider investing, both intellectually and financially, across the gamut of information operations.

New Arsenals, Old Rivalries

Could a small country develop the capability to hit the United States with a long-range unconventional weapon? Most certainly one could, but whether such a state would be inclined to try is an entirely different matter.

The risk is real. Congress learned in 1998, according to "The Report of the Commission to Assess the Ballistic Missile Threat to the United States" [4], that the United States has entered "a new nonproliferation environment" in which there is a far greater availability of ballistic missiles and weapons of mass destruction. As previously mentioned, the report was the work of a private commission headed by Donald Rumsfeld, secretary of defense under President Reagan and the second President Bush.

To begin with, the report refers to a club of renegade nations that appear to work with one another to dodge the strictures of nonproliferation agreements. The states trade with one another and build on the progress of other members of the club to advance their own systems. Indeed, it is arguable that the recent North Korean firing of a Taepo Dong missile was meant to further its own missile development and to serve, in effect, as a marketing demonstration to attract buyers from other countries outside the international nonproliferation framework.

Another factor, the report points out, is that access to information on a global scale keeps growing exponentially, as the bounds of the Internet in particular remain uncharted. What's more, there has been an easing of access to what the Rumsfeld Commission terms the rudimentary technologies that were employed in early generations of U.S. and Soviet missile systems.

There is a fourth factor: the flexibility with which technical personnel from the West, and especially from the former Soviet Union, can move to a potential proliferator. Because so many third world countries now have ballistic missiles of their own and, therefore, are interested in upgrades, whether of guidance or range, they are less pressed to acquire whole systems.

They are also well aware that it is the acquisition of such whole systems that garners the most international attention and is most easily policed by the web of agreements, such as the Missile Technology Control Regime, that the United States and its allies have spun to guard against proliferation. Instead, what many nations are focusing on is brainpower, people who are intimately familiar with technical data packages, who can advise on both long-term improvements and quick fixes, and who can offer recommendations on everything from guidance systems to materials technology to quality control to integration.

Many such scientists and technicians, particularly in the former Soviet states, are willing and eager to improve their material lot by helping renegade nations enhance systems that were often acquired from the Soviet Union or that are derivatives of such systems. Although Western nations recognize the destabilizing impact of peripatetic unemployed scientists working in countries that "show them the money," they can produce few options. Other than propose alternative employment, the United States and its allies have little to offer, particularly to those motivated by ideological or religious ideals. A significant number of missile owners are potential adversaries of the United States, and, many of the third world powers have mutual supranational interests. Should a Muslim nation, for example, be taken over by extremists, it could seek support in other Muslim nations from like-minded elements that might not necessarily have seized power but would be in a position to offer the new regime intellectual assistance and perhaps financial aid.

Certainly, even the availability of resources, and of willing foreign technologists, combined with nefarious intentions, does not in itself suffice for the successful pursuit of a program for intercontinental ballistic missiles. Otherwise, Libya would long ago have been in a position to threaten the United States. Nevertheless, the ability of lesser powers to mount such a threat over the next two decades cannot be ruled out.

Furthermore, as the recent North Korean and Iranian missile tests demonstrated yet again, a third world country whose leadership is determined to advance its capabilities will not be deterred by nonproliferation regimes. It will find ways to draw upon outside resources in support of its program, and, no less important, it will do so well in advance of the timetables set forth by Western intelligence.

Stolen Thunder Tools

Like a neutron bomb (whose design Chinese agents allegedly stole), the Cox report demolished any doubt that China engages in espionage against the United States (see sidebar, "China Grabs U.S. Technology to Modernize Its Military"), but it left standing a whole array of big questions and small mysteries.

CHINA GRABS U.S. TECHNOLOGY TO MODERNIZE ITS MILITARY

The request to a Massachusetts defense contractor seemed innocent enough: China needed fiber-optic gyroscopes, the latest in navigation equipment, for a new high-speed rail system, the buyers allegedly said. The deal might have gone through if not for a small hitch: the manufacturer recalled that the men, using a different company name, had tried earlier to get a U.S. license to export the gyroscopes to China—and had been turned down.

In 1999, U.S. Customs agents in San Diego arrested a Chinese national named Yao Yi for criminal export violations. Yi has pleaded not guilty; his coconspirator, Collin Shu, a Canadian, was also arrested and pleaded not guilty. The two are accused of conspiracy to illegally export items designed for military purposes. The gyroscopes are generally used for guiding missiles or maneuvering fighter jets. To put these in a train is like putting an F-14 engine in a Cessna.

Intense Debate

The gyroscope case is one of the latest incidents illuminating Beijing's voracious appetite for high-end U.S. technology that has military capabilities. Also in 1999, a man was arrested in Detroit for allegedly trying to illegally ship to China a riot-control vehicle. A report by a panel chaired by Rep. Christopher Cox (R-Calif.), in 1999, suggested that China may have married U.S. computer technology with nuclear weapons designs it stole in the 1980s from U.S. labs. The report presented no

→

hard evidence of this, but it will almost certainly add fuel to an already intense debate over exports of high-speed computers to Beijing.

Proponents of the sale of high-tech goods to China say they help open the country to influences like American television shows beamed off U.S.-manufactured satellites. They add that U.S. electronics firms need foreign markets like China if they are to stay healthy in the face of stiff foreign competition.

The present and past administrations have generally supported this view, but in 1999, in a surprising turnaround, Clinton advisers blocked California satellite maker Hughes Electronics Corp. from sending two $670-million satellites to be launched in China. Various officials offered different explanations for the decision, but the government told Hughes the launches could transfer too much militarily significant know-how.

Critics of high-tech exports to China say they have other concerns as well: the same technology that is already turning China into a land of ATM machines and cell phones could help the People's Liberation Army begin to master IW. Pentagon officials counter that nobody is assessing the impact of the fiber-optic lines, electronic-switching gear, computers, and satellites pouring into China. Some examples follow.

In March 1996, as Beijing was threatening Taiwan with missiles, the State and Defense departments approved the export to China of two satellite receiving stations worth $7.3 million. The recipient, documents show, was China Electronic Systems Engineering Company, part of China's military. The stations came equipped with ports to plug in Chinese-made encryption devices. The National Security Agency signed off on the deal, but congressional critics say the sale deserves a second look.

China buys nearly half of the supercomputers the United States exports to high-risk countries. Experts point out that the Chinese can evade U.S. export controls by harnessing together less powerful machines—or buying high-capacity machines on a Russian Internet site. Industry groups plan to lobby Congress to allow more powerful machines to be exported, arguing that 1995 limits are already outdated. The Cox report calls for greater scrutiny, including spot checks in China to ensure the best machines are used only for civilian purposes. There are two trains rushing down the track directly at each other on this.

Experts say China's rapidly modernizing military is still years from catching up with the United States, at best, but some worry that China will put high-tech imports to their best military uses and turn into a surprising adversary.

The most sensational charge in the 872-page Cox report—that China has obtained secret data on every warhead in the U.S. nuclear arsenal—is based on a single document that a Chinese agent deliberately fed the CIA in 1995. Why would China's spy masters tip their hand? Maybe they bungled, giving away too much in an effort to plant a double agent. Maybe they were warning Washington to butt out of China's touchy relationship with Taiwan, or maybe, they were just following the 1,500-year-old advice of the military philosopher Sun Tzu to "sow confusion in the enemy's camp."

The release of the bipartisan Cox report in 1999 certainly did that. Its overall conclusions are chilling. For two decades, it says, China has used spies, front companies, and scientific exchanges to filch some of America's most precious secrets, but on closer reading, it is still unclear how much damage has been done to U.S. national security. In most cases, it seems, Beijing got helpful hints, not blueprints.

Democrats on the congressional panel, which was led by Republican Rep. Christopher Cox of California, unanimously approved the report, but they also questioned its alarmist tone. There are, unfortunately, a number of places where the report reaches to make a point and, frankly, exaggerates.

On the other hand, concrete advances from spying sometimes don't show up in weapon systems until years later. It's possible, as Cox and some Pentagon officials argue, that the sum of China's technological thievery is even larger than its parts. So how worried should Americans be? Here's what the report does and does not say:

Nuclear Warheads

China stole classified design data on the W-88, a miniaturized nuclear warhead that is the most advanced in the U.S. arsenal. The CIA discovered this in 1995 when a Chinese "walk-in" (an agent who came forward voluntarily) handed over a Chinese document stamped "secret." The unclassified version of the report does not reveal the contents of the document, but an administration official at the time said it contained two quite specific and detailed bits of data on the W-88. One was the size of the "package" containing the nuclear device, whose yield (explosive power) was already available from open sources. Although useful, that knowledge is a far cry from a detailed plan for a nuclear weapon. It's more like looking at a car's engine compartment and knowing how much horsepower the block can produce.

Because the CIA later determined that the walk-in was a double agent acting on the orders of China's intelligence service, it is unclear whether the Chinese had already milked the information or never considered it all that important. The Chinese document, dated 1988, also described the size and yield of four other U.S. warheads, but that may have come from publicly available sources.

Why does China covet America's nuclear secrets? The Cox committee concluded that U.S. technology would help China build smaller warheads to sit atop a new generation of lighter, mobile missiles, but the upgrade has been in the works for 23 years. Most experts think that its goal is to ensure China's "second-strike capability"—the ability to retaliate for a nuclear attack, not to launch a first strike.

Beijing's leaders have good reason to worry about the reliability of their current strategic-missile force: fewer than 20 aging, 1950s-era rockets.

The first of the new missiles, the DF-31, won't be able to reach most of the territory of the United States, but could it intimidate China's neighbors or make the United States hesitate to defend Taiwan in a crisis? Definitely.

Rocket Technology

The Cox panel was established partly to look into allegations that two U.S. aerospace firms, Hughes and Loral, helped China improve the reliability of its Long March booster rockets. The report says the two companies ignored restrictions on technology transfers and gave away sensitive information while helping China investigate a series of failed attempts to launch the firms' satellites into space.

What, exactly, did Chinese scientists learn? How to build better "fairings," the nose cone that protects the satellite during launch. How to compensate for the violent winds that buffet rockets in flight. How to fix the Long March 3B's guidance system. How to better investigate failed launches. This information has improved the reliability of Chinese rockets useful for civilian and military purposes.

Still, it is unclear how quickly China will be able to make those improvements. In the past, China has sometimes had difficulty absorbing Western technology. The spying and technology transfer is of enormous concern, but, having it in your hand doesn't mean you know how to use it or effectively deploy it.

Computers

There is no mystery about how China got advanced computers. The question is what it does with them. Under relaxed export rules, China has legally bought 1,236 high-speed, American-made computers since 1996. The Cox report says they have been used in nuclear weapons applications, such as modeling hypothetical explosions rather than conducting real ones after Beijing signed the Comprehensive Test Ban Treaty in 1996. The congressional panel recommended spot checks to monitor the use of U.S. computers in the future, rather than cutting off sales.

Radar

The Cox report also asserts that classified U.S. radar research stolen by the People's Republic of China could be used to threaten U.S. submarines, but the White House produced a letter from the Navy to the Justice Department stating, It is difficult to make a case that significant damage has occurred from the alleged disclosure.

China has never aspired to a large nuclear arsenal. One possible explanation for Beijing's disclosure of its own espionage is that Chinese leaders wanted the world to know they could build a large, modern arsenal—if they wanted to. It's deterrence on the cheap. If that was the plan, it just might have worked.

WHY TOOLS ARE EASY TO GET AND USE

Why are hacking and IW tools and weapons of mass destruction easy to get and use? Easy answer: They can be stolen.

For example, investigators at Los Alamos National Laboratory, in 2000, discovered that computer hard drives containing nuclear weapons data and other highly sensitive material stored in a vault at the laboratory had disappeared, according to several United States Government officials. The hard drives were stored in locked containers inside a vault in the nuclear weapons division of the national laboratory. Officials reported that the hard drives were missing on June 1, 2000, after officials went to search for them following forest fires in the area. The containers remained in the vault, but the hard drives were gone.

The material, stored in the vault of the laboratory's X Division, where nuclear weapons are designed, contained what officials described as nuclear weapons data used by the government's Nuclear Emergency Search Team, or NEST, which responds to nuclear accidents and nuclear-related threats from terrorists. The material includes all the data on American nuclear weapons that the team needs to render nuclear devices safe in emergencies. In addition, the missing material included intelligence information concerning the Russian nuclear weapons program.

The Energy Department's security czar at the time, Eugene E. Habiger, conducted an intensive search and investigation at Los Alamos but did not find the data. He has written a secret report on the matter, and the FBI has been brought in to assist with the investigation. Officials said they remained uncertain whether the data has been misplaced or stolen.

This disappearance of the nuclear weapons data represents a major embarrassment for a laboratory that had already spent the past year under scrutiny for lax security in connection with the Wen Ho Lee case. As previously mentioned, Dr. Lee was a scientist at Los Alamos who was fired in March 1999 for security violations after being the subject of a counter-intelligence investigation that looked into evidence that China had stolen American nuclear secrets. Dr. Lee was never charged with espionage, but after he was dismissed, investigators accused him of downloading and copying vast amounts of secret nuclear weapons data from a secure computer at Los Alamos into an unclassified computer network and onto portable tapes. Dr. Lee was arrested in December 1999 on charges of mishandling classified material.

The discovery of Dr. Lee's unauthorized downloads in April 1999 prompted then Energy Secretary Bill Richardson to order a shutdown of the lab's computer systems, while mandating security training sessions for Los Alamos employees. Congress later passed legislation creating a new nuclear weapons agency within the Energy Department to oversee Los Alamos and the nation's other nuclear weapons laboratories. The new security breach is believed to have occurred long after Dr. Lee was dismissed.

Energy Department officials indicated that they notified the FBI as soon as they discovered that the material was missing, but some law enforcement officials say that officials at the lab downplayed the fact that the data was missing from the vault and assumed that the hard drives would turn up somewhere else in the lab. The officials are said to have assumed that the material was in use somewhere in the lab by Los Alamos scientists. The fact that the missing data included intelligence reports has led law enforcement officials to become skeptical that the material was simply misplaced. The hard drives were eventually found near a trash-can. Questions remain: Who took them and how much classified material was downloaded before they were eventually found?

WHY NASTY PEOPLE ARE SO HARD TO TRACK DOWN AND CAPTURE

When a pair of suicide bombers crippled the destroyer *USS Cole* in a Yemeni port in mid-October 2000, killing 17 American sailors, top U.S. counterterrorism officials had a fearful intuition: This is revenge for Albania. In mid-1998, the CIA, working with Albania's intelligence service, had rolled up a terrorist cell guided by wanted dead or alive Saudi exile Osama bin Laden. A deadly bombing of the U.S. Embassy in Albania's capital, Tirana, was barely averted. The Middle Eastern plotters were sent home to face prosecution. They have not forgotten that, and they're still looking for payback.

The United States has yet to nail all of those responsible for the *Cole* attack (even though a few suspects have been detained), but that first guess made a macabre sort of sense to those waging the interminable war against terrorism. Few Americans realize the full extent and intensity of what has become an around-the-clock, across-the-globe campaign against fundamentalist Islamic terrorists, a confusing web of groups and names fused only by their hatred for the United States and, often, their shared experience fighting the Soviet Union's occupation of Afghanistan in the 1980s.

This war is waged largely in the shadows, a cat-and-mouse contest between terrorists and intelligence agencies that only rarely comes into public view. Much of the vast U.S. national security machinery (and a ballooning budget) is trained on the threat. Fragmentary bits of data gleaned from eavesdropping satellites, human informers, friendly governments, and old-fashioned police work are pieced together to deter and disrupt terrorist attacks on a regular basis.

High Alert

Recently, U.S. intelligence agencies warned that U.S. naval forces in Italy and the airbase in Incirlik, Turkey, were being targeted. The posts went on high alert, and the aircraft carrier *USS Truman* was diverted from Naples to Crete. Meanwhile, the State Department sent a global alert to all its posts, ordering them to review security procedures.

The war comes out of the shadows when U.S. intelligence and law enforcement agents lose a battle, such as in the *Cole* attack or the 1998 bombings of two U.S. embassies in East Africa (see sidebar, "Putting Terror Inc. on Trial"). As traumatic as they are, though, for each such loss there is many an unheralded success—dashing terrorists' hopes of more bloodied bodies and battered buildings on the world's TV screens.

PUTTING TERROR INC. ON TRIAL

Ali Mohamed is a man of many faces: Egyptian intelligence agent, U.S. Army paratrooper, FBI informant, and aide to wanted dead or alive terrorist mastermind Osama bin Laden. Before bombs shattered U.S. embassies in Kenya and Tanzania, Mohamed says, he scouted possible targets and personally brought bin Laden photos of Nairobi sites. Bin Laden looked at the picture of the American Embassy and pointed to where a truck could go as a suicide bomber.

Mohamed, 51, is now poised to play a new role—as the Justice Department's star witness in the long-awaited trial of bin Laden's alleged followers, which started in January 2001 in New York City. A sweeping 319-count indictment charges bin Laden and 20 others with a terrorist crime spree dating back to 1991. Among the charges: bombings, perjury, and conspiracy to murder Americans around the globe. The attacks include not only those on the U.S. embassies in 1998 (which left over 220 dead and 5,000 injured), but also attacks on U.S. troops in Somalia and Saudi Arabia. Although bin Laden remains at large (with a $100 million U.S. reward on his head), five of those indicted are now in U.S. custody—as is Mohamed, who pleaded guilty in October 2000.

INFIDELS

The October 2000 suicide bombing of the *USS Cole* and the 9-11 attacks (tied by investigators to bin Laden's network) have added fresh urgency to the government's efforts to thwart the wanted dead or alive Saudi exile, now hiding in the badlands of Afghanistan or nearby in Pakistan. Led by Mohamed's likely testimony, the trial promised an unprecedented look at America's most wanted terrorist and at al-Qaeda, the fanatic organization that he guides. The indictment imparts an image of a paranoid, virulently anti-American network determined to purge Muslim lands of "infidels." To achieve this, bin Laden's men strove to obtain chemical and even nuclear weapons, according to prosecutors.

→

Proving a grand conspiracy may be difficult. Prosecuting international terrorists is often a delicate balance between law enforcement's need for evidence and the intelligence world's need to protect sources and methods. Through electronic eavesdropping, for example, U.S. officials quickly learned of bin Laden's involvement in the embassy blasts, but they are loath to introduce such sensitive records into court.

Holy War

Such concerns may explain the indictment's at times tenuous links among the alleged terrorists. Prosecutors tie bin Laden to the conspiracy largely through his funding of al-Qaeda and his calls for holy war against the West. For some defendants, their work with al-Qaeda appears to be enough. For others, it is their work in bin Laden's businesses in Sudan, from construction and agriculture to an investment house, which prosecutors call fronts for terror. Still others are tied to al-Qaeda's ruling council, where terrorist plots (like the 9-11 attacks) are said to be hatched.

With his guilty plea, Mohamed has made the prosecution's job far easier. Under oath, Mohamed already has done more than tie bin Laden directly to the embassy bombings. He strongly hinted he could connect the dots to the five others in custody, who have all pleaded not guilty.

Two of the defendants, Mohamed Rashed Daoud al-Owali and Khalfan Khamis Mohamed, face the death penalty if convicted, as prosecutors have the strongest evidence tying them to the embassy attacks. Al-Owali, a Saudi Arabian, allegedly filmed a statement before the bombing celebrating his "martyrdom," and rode in the pickup carrying the Nairobi bomb; he was found later in a hospital with keys to the truck's padlock nearby. Prosecutors say Khalfan Mohamed, a Tanzanian, helped grind up TNT and load the truck used in the Dar es Salaam bombing. A third defendant, Saddiq Odeh, a Jordanian, is allegedly tied to TNT and detonators used in Tanzania.

A fourth man, Mamdouh Mahmud Salim, allegedly purchased the 1998 Toyota Dyna truck that carried the bomb in Nairobi. His case was recently severed from the others after he stabbed a prison guard in the eye. Investigators are hoping a fifth defendant, Wadih el-Hage, will follow Ali Mohamed's lead and cooperate. A tire store manager in Arlington, Texas, he acted, prosecutors contend, as a bag man and passport fixer while working as bin Laden's personal secretary.

Targets

Ali Mohamed's testimony, which will likely earn him a reduced sentence, may prove particularly damning to el-Hage. Mohamed, a former U.S. Army sergeant, a naturalized American citizen born in Egypt, claims he worked with el-Hage in Nairobi

→

and that during a visit to el-Hage's house, bin Laden's security chief told him to conduct surveillance on American, British, French, and Israeli "targets" in Senegal.

Defense attorneys on the case know they're facing tough odds. Mohamed's guilty plea has thrown a wrench into their strategies. For defendants facing the death penalty, their lawyers' primary focus is to stop them from getting killed. If Ali Mohamed does indeed take the stand, his credibility will likely come under fire. The talkative terrorist has a record of shifting loyalties and admits to lying to investigators in the past.

El-Hage, a naturalized U.S. citizen, certainly seems to be feeling the pressure. Five days after Mohamed's testimony, he suddenly also attempted to plead guilty. The plea, offered without consulting with prosecutors, was thrown out because el-Hage told the judge he was acting not out of guilt, but because he wanted to escape the humiliation of a trial. Should el-Hage decide to flip with prosecutorial blessing, his testimony could offer a trove of information. Court documents place the 43-year-old el-Hage within a rogues' gallery of terrorists. The Lebanese native is allegedly tied not only to the embassy bombs but also to a string of criminal acts, including attempted arms sales to those later convicted in the 1990 murder of radical Rabbi Meir Kahane and the 1993 World Trade Center bombing.

Further revelations may come from Ali Mohamed, who is cooperating with the FBI. Terrorism experts already are pondering his assertion that through the mid-1990s, bin Laden's al-Qaeda maintained close ties to Hezbollah, the Iranian-backed militia, and to Iranian security forces. Al-Qaeda and its allies received explosives training at Hezbollah camps in Lebanon, Mohamed claimed, and received bombs disguised to look like rocks from the Iranians. The implications are troubling. Iran is an untold story in this. How many elements have they kept out of this indictment?

Perhaps several. Ties to the *USS Cole* bombing may well emerge from trial testimony, and a further indictment in New York (this one under seal) names even more alleged bin Laden conspirators. Clearly, the trial will be but one act in an ongoing and altogether grim play.

In November 2000, for instance, authorities in Kuwait, who thought they had radical Islamists under control, got a nasty shock. They uncovered a tiny terrorist cell plotting to bomb U.S. and Kuwaiti facilities and quietly called in the CIA, which helped trace the plot beyond Kuwait's borders. A suspect, Mohammed al-Dosary, led investigators to a desert weapons cache that held 293 pounds of high explosives, 1,450 detonators, and, for good measure, 5 hand grenades. They were in the final stages of casing targets, claims a U.S. official. Even more worrisome, the plotters had helpers in Kuwait's government, one of the closest U.S. allies in the Persian Gulf.

Publicly, the face of the adversary is bin Laden's, but focusing on one man misses the full picture. Bin Laden has tapped into what U.S. officials sardonically call the "Afghan Veterans Association," Arabs who answered the call to holy war against the Soviets two decades ago—at the time, with backing from the CIA. The threat posed by the Jihadist network didn't become clear until five years ago, with the U.S. arrests of those behind the 1993 World Trade Center bombing. That case sounded the first broad alarms that thousands of Arab veterans from the Afghan war had now trained their sights on the West.

Terror Inc.

Bin Laden finances and motivates a "network of networks," co-opting homegrown terrorist groups, from Egyptian Islamic Jihad to the Abu Sayyaf group in the Philippines to the Islamic Movement of Uzbekistan. It's like winding up little dolls and sending them back to their own countries and letting them create their own movements. The United States government was slow to recognize what bin Laden was doing. Bin Laden was doing something much more than spreading the money around.

Without fanfare, Washington in 1999 opened a new front in the war. The strategy: go on the offensive and hound and disrupt terrorist cells wherever they can be found. U.S. intelligence agencies routinely tip off local security services to problems they didn't even know they had. Cells are placed under surveillance or, using a legal process called "rendition," suspects are forcibly returned to their home countries. In Albania, Algeria, Pakistan, Syria, and elsewhere, bin Laden devotees have been booted out, often on immigration charges and with little publicity. More than two dozen suspects have been brought to justice. The war on terror is fought down in the weeds. It's guys talking to their sources, pulling people in for questioning, and digging for telephone records. It's the slow, dirty, grunt police work that goes on every day.

In 2000, the CIA launched the largest counterterror operation in U.S. history, working with counterparts in Jordan and other countries to thwart a multicontinent "terrorist spectacular" during the millennium celebrations. CIA operatives in more than 60 countries pressured, pleaded, and paid local authorities to crack down on Islamic radicals. The message was, It's crunch time. This cost the agency a great deal of money and resources.

Like battling the mythical Hydra, though, an eliminated terrorist cell only seems to regenerate, sometimes in the same place. Bin Laden and his organization, al-Qaeda, are still itching to pull off an attack in pro-Western Jordan, and though U.S. and Kenyan authorities busted up an al-Qaeda operation in Nairobi in early 1998, the victory was only temporary. They immediately came back in. They were able to use the infrastructure that was in place, spin up a new cell, and go after the target. The August 7, 1998, blasts at the U.S. embassies in Nairobi and Dar es Salaam, Tanzania, killed more than 220 people.

Just as sobering is what officials call the "mujahideen underground railroad," a vast effort to move young recruits to terrorist training camps in Afghanistan. An estimated 40,000 recruits have gone to Afghanistan since 1996. Using professionally forged documents and Hotmail Internet accounts to keep in touch, network members move people through Italy, the Balkans, Turkey, and Dubai.

Recruitment

The Finsbury Park Mosque sits in a gritty part of London, not far from the Arsenal soccer stadium. Inside, the only sign of Islamic activism is a hand-made sign protesting Russia's war in Muslim Chechnya, but U.S., British, and Yemeni officials say the mosque is a recruitment station for terror camps and that its fundamentalist imam, Abu Hamza al-Masri, has ties with terror groups abroad.

Often, the process begins when a potential recruit visits a local mosque and makes a small donation. While some of the funds may go to legitimate Islamic charity work, bin Laden receives a steady stream from mosques, charities, and schools. The way to get rich is to come up with a scheme to get everyone to pay you 5 cents a month. That's what he's done. The United States has tried to block the money flow but has made little progress.

Despite the nature of the quarry, progress is being made in the war on terrorism. The United States is certainly holding their own. There's a chance that the United States is even gaining ground, but not very much. Bin Laden's success (due to the 9-11 attacks) has spurred unprecedented international law enforcement cooperation. Jordanian officials alerted U.S. agencies to the millennium threat. Even Russia, which fears radical Islam in Chechnya and Central Asia, now works regularly, if quietly, with U.S. counterparts. This is a dramatic turnaround. Nevertheless, some U.S. agencies still *dropped the ball* in not being able to prevent the 9-11 terrorist attacks.

Through eavesdropping and, increasingly, informants, Western spy agencies are gaining a clearer picture of the structure of bin Laden's network and his inner circle, but penetrating the distinct cultures in which the terrorists operate is difficult. The CIA has begun a special program to recruit Muslims, in hopes of worming its way inside. One advantage: the terrorist networks' decentralized structure. They are vast, but they're not real tight. The CIA is more aggressive but is hampered by 1995 regulations restricting recruitment of sources with unsavory backgrounds. The CIA claims the rules don't block operations.

Nor have the terror fighters been able to get bin Laden himself, who still moves between homes, residences, and underground bunkers in Afghanistan or in neighboring Pakistan. He is protected by what a Pentagon official calls "double walls of security."

One is provided by his dwindling Taliban hosts, and his own personal security detail includes an elder son who is said to rarely leave his side but now is presumed dead.

> NOTE
>
> *Recently, terror fighters were further embarrassed by the elusiveness of bin Laden, when he showed up at his elder son's wedding in full view of international media cameras.*

The terrorists do their own spying. They do exploit our weaknesses. The *Cole* attackers slipped through a small window (four hours every other month) as U.S. ships refueled in Yemen. They hit the United States in exactly the right place. Sometimes, terrorists dispatch walk-ins, "informers" who proffer false information to U.S. agents. Bin Laden previously used an INMARSAT satellite telephone—on which U.S. spy agencies eavesdropped and quickly established his role in the East Africa bombings. When that fact became public, he switched to a system of mule messengers and code words.

Still, U.S. high-tech wizardry plays a key role in combating terrorists who are increasingly high-tech themselves. When Khalil Deek was arrested in Pakistan in December 1999, U.S. and Jordanian officials weren't sure how much of the millennium plot they'd unraveled. Deek (who denies involvement) had computer files locked with a commercially available encryption program. U.S. agents rushed the computer to the Fort Meade, Maryland, campus of the code-breaking National Security Agency. It was a race against time. The National Security Agency had to know whether Deek had operational information such as where and how the attacks were planned.

That threat was thwarted, but others keep coming: an average of 40 each week, according to the FBI. Fighting terrorism is like being a soccer goalie. You can block 99 shots, but you miss one and you lose the game.

THE IW GAMES

The number of cyberattacks and intrusions into Pentagon computer networks in 2004 is expected to top off at 68,000, an increase of 9% from 2003, according to the DoD. However, the overwhelming majority of those intrusions occur because of known vulnerabilities and poor security practices. Ninety-nine percent of the successful attacks and intrusions can be attributed to known vulnerabilities and security gaps that have gone unfixed and poor security practices by defense agencies.

Malicious hackers and other criminals penetrated Pentagon network security at least 76,271 times during the first seven months of 2004. Hackers stung the Pentagon at least 66,366 times in 2003 and 58,493 times in 2002. These incidents will have served a constructive purpose if the Pentagon learns from them. By exposing and highlighting vulnerabilities, the attacks can actually help inoculate the system for times of crisis—but only if the appropriate lessons are learned now.

The number of successful attacks raises questions about the Pentagon's preparedness to withstand more skilled adversaries. The Pentagon is currently operating in a relatively benign international environment, yet they were hard pressed to deal with the detected hacks. The Pentagon has a raging case of technological hubris and is ready to be taken to the cleaners by a savvy adversary.

In addition to weak security practices by DoD network administrators, the increase in the number of attacks can be attributed to the greater availability of sophisticated hacker tools on the Internet. Someone with a very limited amount of computer skills can do a lot of damage. The increase in the number and the sophistication of the attacks poses a significant threat to DoD plans to use computer networks as part of its overall strategy to fight future conflicts, a concept known throughout the Pentagon as "network-centric warfare."

Despite claims by senior officials that DoD's classified systems are immune from attack, there are several connections between the Pentagon's top secret and secret networks and the unclassified network that connects to the global Internet that make them vulnerable. However, sophisticated encryption devices designed by the National Security Agency protect the classified networks. All of the Pentagon's various layers of networks are connected. Regardless of classification, there are connections and the Pentagon is dependent on that infrastructure.

However, legal restrictions have hampered the DoD's ability to respond to attacks and track down hackers. Due to legal and privacy [5] restrictions, the department is prohibited from pursuing hackers beyond its networks. The agency can take defensive measures to stop a hacker, but to actively catch and prosecute a hacker, it must go through the FBI. The agency doesn't go outside of their firewalls, but they'd like to.

One solution that the department is working on is a concept called "legal hot pursuit." Pentagon criminal investigators are searching for a legal framework that would enable them to use one search warrant to track hackers back through the multitude of Web sites they often use as launching pads for their attacks. Today, these investigations require separate search warrants for every system used as part of a distributed denial-of-service attack.

How Other Countries Are Getting into the IW Games

According to the CIA, other countries are developing cyberattack capability. The United States could become a target of cyberattacks from a growing list of terrorists and foreign countries, including Russia, China, and even Cuba (see sidebar, "Has Cuba Joined the IW Games?")

HAS CUBA JOINED THE IW GAMES?

These must be jittery times for anyone in the military who uses the Internet. Not only do they have to guard against Love Bug worms and security holes in Microsoft Outlook, but also they've got to worry about Fidel Castro hacking into their computers.

According to the Defense Intelligence Agency, the 78-year-old communist dictator may be preparing a cyberattack against the United States. Castro's armed forces could initiate an IW or computer network attack that could disrupt the military.

One can say there is a real threat that Cuba might go that route. There's certainly the potential for Cuba to employ those kinds of tactics against the United States' modern and superior military. Cuba's conventional military might is lacking, but its intelligence operations are substantial.

In addition to Cuba, terrorists such as Osama bin Laden are now using the Internet and encryption to cloak communications within their organizations. They recruit people on Internet sites and use encryption. They send their operational planning and judgments using encryption. They raise money. Bin Laden allegedly uses encryption (and a variant of the technology, called steganography) to evade U.S. efforts to monitor his organization. Also, bin Laden and his global network of lieutenants and associates remain the most immediate and serious threat to America.

And what about Castro? It might seem odd to view a country best known for starving livestock, Elian Gonzalez, and acute toilet paper shortages as a looming threat, but the Pentagon seems entirely serious. Cuba is not a strong conventional military threat, but their ability to use asymmetric tactics against the United States' military superiority would be significant. They have a strong intelligence apparatus, good security, and the potential to disrupt the U.S. military through asymmetric tactics. Asymmetric tactics is military-ese for terrorist tactics when your opponent has a huge advantage in physical power.

The CIA is detecting with increasing frequency, the appearance of doctrine and dedicated offensive cyberwarfare programs in other countries. They have identified several countries, based on all-source intelligence information, that are pursuing government-sponsored offensive cyberprograms.

IW is becoming a viable strategic alternative for countries that realize that, in conventional military confrontation with the United States, they will not prevail. For instance, a cyberattack against a national target such as a transportation center or electrical power distribution center would, by virtue of its catastrophic consequences, completely overlap with the use of weapons of mass destruction.

The United States can make the enemy's command centers ineffective by changing their data system. The enemy's headquarters can then be used to make incorrect judgments by sending mis- or disinformation. The enemy's banking system and even its entire social order can also be dominated.

Cyberwarfare represents a viable strategy for countries that are outmanned in conventional warfare. These countries perceive that cyberattacks, launched from within or outside the United States, represent the kind of asymmetric option they will need to level the playing field during an armed crisis against the United States. With the advent of the cyberthreat, the United States is faced with the need to function in the medium of cyberspace, where it will conduct its business in new and challenging ways.

The technology to launch cyberattacks is already well known. The same means that the cybervandals used recently (in a much-publicized denial-of-service cyberattack that temporarily shut down several large Web sites) could also be used on a much more massive scale at the nation-state level to generate truly damaging interruptions to the national economy and infrastructure.

Both the Chinese and Russians have expressed interest in some form of international effort to place curbs on such attacks. The Russians have gone so far as to formally propose via the Secretary General of the United Nations the development of an international legal regime to combat information crime and terrorism. Organizations such as Interpol have the structure in place to facilitate in sharing IW data between countries, but a common basis of legislation, policy, and procedures is still needed.

SUMMARY

Terrorists and rogues have often targeted the United States. They attack American interests and citizens abroad because of the wealth of opportunities, the symbolic value, and the exposure from the world's most extensive news media. Because of its role in American power projection, the Air Force can be a target, as with the bombing of Khobar Towers, the USAF barracks in Dhahran, Saudi Arabia.

The Air Force has also been called on to counter the IW arsenal and tactics of terrorists and rogues, as it did in striking targets in Afghanistan and Sudan after the August 1998 bombing of U.S. embassies in Kenya and Tanzania. Highly publicized attacks such as the World Trade Center bombing, the use of chemical weapons in the Tokyo subway, and Hamas suicide attacks in Israel have led some to argue that terrorism is an increasing threat.

Others point to "cyberterror," weapons of mass destruction, or other alarming scenarios. A multifaceted Project AIR FORCE (PAF) study put such issues in strategic perspective, tracing the evolution of international terrorism against U.S. civil and military targets, identifying key trends, and proposing strategies for containment.

Although this is not an issue for the Air Force alone, this chapter recommended a number of specific steps that could better prepare the U.S. military and private companies to confront "the new terrorism" and its IW arsenal and tactics, as follows.

Conclusions

- The past decade has seen extraordinary change in the international security environment, yet much discussion of terrorism remains tied to images from previous epochs; it assumes the same kinds of actors using a new and more threatening arsenal of weapons.
- The PAF team found that changing technologies and tactics accompany equally important changes in the motives and structure of terrorism itself. These underlying changes are making terrorism more lethal. Although the number of incidents worldwide declined during the 1990s, the number of fatalities rose.
- Several factors account for this new lethality. Some terrorists believe that ever more spectacular and lethal acts are necessary to capture public attention.
- Terrorists have also become more adept at killing, with deadlier weapons made more easily available through alliances with rogue states and private sponsors. During the 1980s, for example, Czechoslovakia reportedly sold over 40,000 tons of Semtex, a plastic explosive, to countries sponsoring international terrorism. Assistance from such governments often enhances the capabilities of terrorist groups.
- With bomb-making and other information now widely available, the number of "amateur" participants has increased. They can be just as deadly as their professional counterparts and, without a central command authority, both harder to anticipate and less concerned about indiscriminate casualties.
- A final trend is perhaps the most striking: the rise of religiously motivated terrorism has brought increased lethality. In the 1960s and 1970s, when modern international terrorism arose, it was motivated almost exclusively by ethnic, nationalist-separatist, or ideological causes. This began to change in the 1980s, and since then a significant share of terrorist groups has been motivated at least partly by religion. Such groups are an important force behind terrorism's rising lethality, presumably justified in the terrorists' minds by the transcendent cause.
- In 1996, for example, the year of the Khobar Towers attack, religiously motivated terror accounted for 10 of the 13 extremely violent and high-profile acts that took place worldwide.
- Counterterrorism today requires diverse responses to an increasingly diverse challenge.
- Mainstream ethnic, separatist, and ideological groups will deviate little from established patterns. They will largely rely on the gun and the bomb, as they have for a century. The sophistication of their weapons will be in their simplicity:

clever adaptation of technology and materials that are easy to obtain and difficult to trace.

- State-sponsored terrorism has been the most conservative in terms of tactics; almost without exception these acts have been carried out with a conventional arsenal of weapons. New entities with systemic, religious, or apocalyptic motivations and greater access to weapons of mass destruction may present a new and deadlier threat.
- High-tech weapons and nuclear materials from the former Soviet Union are increasingly available, and chemical and biological warfare agents are easily manufactured.
- Amateurs, in particular, who may be exploited or manipulated by professional terrorists or covert sponsors, may be willing to use these weapons.
- In addition to becoming more lethal, the terrorist threat is changing in another dimension as well—one driven by computer and communication networks. The most striking development here is not attacks on America's information infrastructure. It is the way that terrorists are organizing themselves into new, less hierarchical networks and being sponsored by secret, private backers. This change, enabled by the information revolution, makes detecting, preventing, and responding to terrorist activity more difficult than ever before.
- Analysis of terrorist organizations in the Middle East also suggests that the more active and lethal of these make extensive use of IW techniques.
- Future terrorism may often feature information disruption rather than physical destruction. PAF found that many terrorist entities are moving from hierarchical toward information-age network designs.
- Terrorists will continue using advanced information technology to support these organizational structures.
- More effort will go into building arrays of transnationally internetted groups than stand-alone organizations. This is likely to make terrorism harder to fight.
- Hierarchies in general have a difficult time fighting networks. There are examples across the conflict spectrum, including the failings of governments to defeat transnational criminal cartels engaged in drug smuggling and narcoterrorism, as in Colombia.
- The persistence of terrorist movements, as in Algeria, in the face of unremitting state opposition, also shows the robustness of the network form, including its ability to spread to bases in Europe.
- Arrests in the United States just before New Year's Eve 1999 suggest the ability of such networks to operate across regions. The PAF study notes that this change is part of a wider move away from formally organized, state-sponsored groups to privately financed, loose networks of individuals and subgroups that may have strategic guidance but enjoy tactical independence.
- Conventional counterterrorism techniques may not work well against such groups.

- Retaliation directed at state sponsors, for example, may be effective against traditional terrorist groups but will be likely to fail against an organization with multiple, dispersed leaders, and private sources of funding.
- Implications for the Air Force: how can the United States respond to more lethal, more diverse, and increasingly privatized patterns of terrorism?

An Agenda for Action

The United States needs to formulate a clear, realistic, and realizable national strategy that can evolve with the changing terrorist threat. The PAF team identified four core elements to that strategy: reducing systemic causes, deterring terrorists and their sponsors, reducing the risk of "superterrorism" such as attacks involving weapons of mass destruction, and retaliating where deterrence fails. This strategy leads to key implications for the use of air- and space-based assets.

With its increasing lethality, possible access to weapons of mass destruction, and the shift to flexible and robust network organization, terrorism is a more formidable problem than ever before. Air and space power will be critical elements in defending U.S. interests—including U.S. Air Force forces—against this evolving threat.

The U.S. government needs to set an agenda for action that goes beyond the work already done in preparation for defending against the IW arsenal and tactics of terrorist and rogues. With the preceding in mind, when completing the Information Warfare Arsenal and Tactics of Terrorist and Rogues Checklist (Table F15.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for networks. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? The past decade has seen extraordinary change in the national security environment.
2. True or False? The PAF team found that changing technologies and tactics accompany equally important changes in the motives and structure of terrorism itself.

3. True or False? Terrorists have become more adept at killing, with deadlier weapons made more easily available through alliances with rogue states and private sponsors.
4. True or False? Counterterrorism today requires diverse responses to a decreasingly diverse challenge.
5. True or False? Mainstream ethnic, separatist, and ideological groups will deviate quite a bit from established patterns.

Multiple Choice

1. The United States faces an increasingly wired but dangerous world, as evidenced by the following, except:
   A. Few countries have programs to develop cyberattack technologies and could develop such capabilities over the next decade and beyond.
   B. The U.S., Russia, China, France, and Israel are developing cyberarsenals and the means to wage all-out cyberwarfare.
   C. Terrorist groups are developing weapons of mass destruction.
   D. Russia has become a breeding ground for computer hackers. The Russian equivalent of the U.S. National Security Agency and organized crime groups recruit the best talent.
   E. Electronic stock scams, robberies, and extortions are proliferating.
2. You can wage successful warfare if you can do the following, except:
   A. Shut down Halliburton
   B. Shut down the United States' financial system
   C. Shut down the transportation system
   D. Cause the collapse of energy production and distribution systems just by typing on a computer
   E. Cause links to globalization to break down
3. The past decade has seen extraordinary change in:
   A. Information attacks
   B. International terrorism
   C. State sponsors
   D. International security environment
4. The PAF team found that changing technologies and tactics accompany equally important changes in:
   A. The line agency and departments
   B. Unneeded capabilities
   C. Special resources that might be mobilized if an international incident occurs

D. Ongoing analysis and research efforts
E. The motives and structure of terrorism itself

5. Terrorists have also become more adept at killing, with deadlier weapons made more easily available through alliances with:

A. Political, ethnic, and religious groups
B. Organized crime
C. Law enforcement organizations
D. Rogue states and private sponsors
E. Individuals empowered by information technology

Exercise

A public institution was the victim of a hacker. The subject got into the network and placed several large media files on several computers and changed the desktop configurations. Management decided against calling law enforcement initially (because of media attention) and instructed the IT department to get a CFS to privately investigate. How did the CFS go about conducting the investigation?

HANDS-ON PROJECTS

A local lumber company went up in flames in late September. The fire safe where they kept their backups had been left open that night after closing. A CFS team (CFST) received three backup tapes and the hard drive from the system. How did the CFST go about conducting their examination?

Case Project

In a U.S. Appeals case concerning email retrieval, the plaintiff used basic recovery and was only able to recover 269 emails in five and a half months. The plaintiff claimed that if there were no responsive emails for 10/04–12/04, it was either because there were no responsive emails from that date or because they did not exist on the accessible backup tapes. How did the CFS that was hired go about retrieving the emails?

Optional Team Case Project

With help from a CFS, a high-quality large-format imaging firm recently won its case against a former general manager and an investment banker. Prior to leaving the format imaging firm to form his own digital imaging company with his codefendant, the defendant emailed the format imaging firm's customer database to his home computer in an attempt to steal intellectual property. They firmly denied the allegations put forth by the format imaging firm, believing that no one would find out since they had deleted the email and the attachment containing the customer database from their home computer. How was the CFS able to go about conducting the email and database recovery?

REFERENCES

[1] Vacca, John R., *Satellite Encryption*, Academic Press, New York, 1999.

[2] Vacca, John R., *Firewalls: Jumpstart for Network and Systems Administrators,* Elsevier Digital Press, Burlington, MA, 2004.

[3] Vacca, John R., *Electronic Commerce,* 3rd ed., Charles River Media, Hingham, MA, 1999.

[4] "The Report of the Commission to Assess the Ballistic Missile Threat to the United States," Pursuant to Public Law 201, 104th Congress, [Members of the Commission to Assess the Ballistic Missile Threat to the United States were nominated by the Speaker of the U.S. House of Representatives, the Majority Leader of the U.S. Senate and the Minority Leaders of the U.S. Senate and the U.S. House of Representatives: The Honorable Donald H. Rumsfeld, Chairman, Dr. Barry M. Blechman, General Lee Butler, USAF (Ret.), Dr. Richard L. Garwin, Dr. William R. Graham, Dr. William Schneider, Jr., General Larry D. Welch, USAF (Ret.), Dr. Paul D. Wolfowitz, The Honorable R. James Woolsey and appointed by the Director of Central Intelligence], (*http://www.house.gov/hasc/testimony/105thcongress/BMThreat.htm*), July 15, 1998.

[5] Vacca, John R., *Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan*, McGraw-Hill, New York, 2001.

16 The Information Warfare Arsenal and Tactics of Private Companies

Although the military establishment has put in place certain safeguards from information warfare (IW) attacks, the state of preparation of private companies is way behind. Even though the military has some responsibility in relation to its own affairs, some responsibility must lie on the private sector. In addition to the private sector having its own interests in reducing vulnerability in cyberspace, the integration of military and private sector interests in the information revolution demand it.

IW of a sort is by no means a new issue for the private sector. Unscrupulous companies have always been delighted to take advantage of new opportunities to sabotage or steal from a dangerous competitor. The development of information networks and vulnerable points of attack merely emphasizes this and increases the opportunities. In addition to industrial espionage activities, internal moles or disaffected employees may destroy information networks, and outside groups such as political activists can also cause significant damage.

NOTE

Economic and industrial espionage is a global industry with a growing workforce.

Private corporations are just as dependent on the infrastructures that form the basis for modern economy—such as telephony, computer networks, electric power, energy and transportation networks—as are military organizations. Various aspects of society are being transferred to cyberspace:

Informational activities: For example, educational activities, processes and results of research, engineering designs and industrial processes, and mass information and entertainment media, in addition to private and public records. Often the electronic version is held in preference to and in the absence of paper records.

Transactional activities: Commercial business, financial transactions, and government activities are now being carried on via computer networks, especially in the absence of paper records.

Infrastructure activities: Physical and functional infrastructures are increasingly being controlled by electronics and software rather than mechanical or electrical means.

Such information is vulnerable to both intentional and unintentional attacks. In addition, the distinctions between warfare, crimes, and accidents are increasingly blurred yet all may have the same damaging results. There are three general categories of attack, especially applicable to a private enterprise:

- Data destruction
- Penetration of a system to modify its output
- System penetration with the goal of stealing information or sensitive data

The means to mount such an attack are by no means difficult to come by. Programs are available free of charge on the Internet to crack passwords or grab key strokes to recognize them, and there is commercially available software to exploit network file system applications that allow file sharing. An increase or the opening of a too large number of sessions in a given time can crash or disable a computer. A user or a system may be disabled by “bombing” it with identical and repeated messages and attached files. There is also a means of attack known as “spamming”—sending numerous emails to a large number of users that can overload a system.

Because of the nature of the competitive market, various programs may be released without proper assessment or testing, which may leave exploitable gaps.

Also, the collapse of the former Soviet Union into what could be termed a “transnational kleptocracy” has led to some fundamental changes in the international security environment:

- Large numbers of unemployed, underemployed, or otherwise disaffected security and KGB operators are now available for hire.
- Large numbers of highly trained and professional scientists and computer experts may no longer have jobs.
- Some countries into which the former Soviet Union (FSU) disintegrated have a nuclear capability or reserves of highly enriched uranium.

- Some estimates claim that 73% of the Russian economy is under the control of criminal enterprises. These enterprises have spread beyond the borders of any particular state.
- Estimates claim that 89% of Russian banks are under criminal control.
- Certain Russian "power ministries" may no longer be serving the interests of the State.
- Russian organized crime has been identified, in particular, in the following transnational areas: money laundering, drug trafficking, and commercial fraud.

It must be stressed that at this stage, Russian organized crime (ROC) is in what could be termed a "nascent state." Although it holds much sway in Russia, ROC has yet to reach a truly transnational existence.

Furthermore, the interplay of corporations and private enterprise with avowed terrorist groups should not be underplayed. Here a problem arises: if a terrorist organization has an identifiable and compassing ideology (or proto-strategy), such an ideology would be general in nature. Also, such an ideology would directly establish broad principles, rather than issues that would provide analysts with a solid foundation.

The artificial and superficial equilibrium imposed by the Cold War has been destroyed, and that ROC and FSU instability needs to be added to the countries that have always used terrorism as a form of diplomacy and an adjunct to their foreign policies. In this new world disorder, smaller states can gain access to a much cheaper form of diplomacy in the use of terrorism—either state sponsored or state condoned.

New and dangerous players have emerged in the international arena. The level of instability and concomitant violence is further heightened by the rise to international political significance of non-state actors willing to challenge the primacy of the states. Whether it be the multinational corporation or a terrorist group that targets it, both share a common characteristic. They have each rejected the state-centric system that emerged 175 years ago at the Congress of Vienna.

All these factors have accelerated the erosion of the monopoly of the coercive power of the state as the disintegration of the old order accelerates. This process in all probability, gains even greater momentum because of the wide-ranging and growing activities of criminal enterprises. These enterprises include everything from arms traders to drug cartels, which will provide and use existing and new weapons in terrorist campaigns as a part of their pursued profit and political power.

In sum, present and future terrorists and their supporters are acquiring the capabilities and freedom of action to operate in the international jungle. They move in what has been called the "gray areas," those regions where crime control has shifted from legitimate governments to new half political, half criminal powers. In this environment, the line between state and rogue state, and rogue state and criminal enterprise will be increasingly blurred. Each will seek out new and profitable targets through terrorism in an international order that is already under assault.

> NOTE
>
> *There is an appreciation that the multinational corporation shares a common characteristic with terrorists, that is (to a certain extent) a rejection of the state-centric system. This rejection is by no means complete (both corporations and terrorists exist at a substate level to some degree). The corporation may seek the protection of the law of a state, and many terrorist organizations will rely on the protection and assistance of states—whether it's overt, or semiovert, or more covert.*

Although some might argue that multinational corporations and terrorist groups stand at either end of a spectrum, the spectrum would still be that of a movement away from "state-centrism" and the concentration of coercive power in the state—with the danger that they each move so far away from one another and that they meet up again. Any ambivalence in allegiance or identification on the part of a non-state quasi-criminal or terrorist organization toward a corporation could easily find its way into violent activity directed at the multinational corporation. Such an ambivalence (and an appreciation of the vulnerability of a corporation) would be brought to the fore, were a corporation to hire the same cyberterrorists to undermine its competitors. A corporation willing to use such agents and to expose its insides to them puts itself at their mercy should the flow of money dry up or should the cyberterrorists then sell their services to a competitor or another organization that bids higher. In addition, the multinational corporation, through its simultaneous existence on many planes of definition, can at any time be seen to be on a similar plane with a substate or non-state actor, as well as being on a nation-state plane—thus attracting criticism and violence that would have been directed toward the identifiably "official" organs of the nation-state in previous times.

As potential targets continue to be hardened in urban areas, the visible aspects of multinational corporations are strengthened and protected. At this point, activities may then move to rural or less protected areas.

Many multinational corporations have now "desegregated their operations" (to borrow a term from another context) and have placed various aspects of their operation in different geographical areas (and even different countries). A failure to strengthen and protect a particular part of that operation may cause incalculable damage to a multinational corporation's network should a weak network node be attacked and disabled.

Overview of Defensive Tactics Private Companies Can Use

This section deals with some technical issues relating to attacking computer and information networks and defensive measures that private companies can take in stopping or hindering attacks. This section will also briefly cover some discrete problems that may be encountered in applying traditional forms of risk treatment to what is essentially a new form of risk, and it will then discuss the possible need for a new or revised approach to the risk-management system of a corporation in light of the new form of threat represented by computer terrorism. It will also discuss what has become known as "information peace-keeping" (IPK). The three elements of IPK are

- Open source intelligence
- Information technology
- Electronic security and counterintelligence

Interestingly, IPK must rely almost entirely on the private sector for sources and services that will require the development of a new national intelligence and secure approach to take into account what has hitherto been an area in which the private sector has not participated. Perhaps the most important aspect of information operations in the 21st century is that it is not inherently military; instead, civilian practitioners must acquire a military understanding and military discipline in the practice of information operations if they are to be effective. This is known as the enmeshing phenomenon.

NOTE

Information peacekeeping is the exploitation of information and information technology to achieve national policy objectives.

Common to all aspects of information operations (IPK, IW, and all source intelligence) is open source intelligence. This means that the involvement of the private sector will become more critical in defense terms in the 21st century. Along with this must go an increasing identification of the private sector with the defense establishment, both in its own perception and in the perception of outsiders. IPK is not

- Application of information or information technology in support of conventional military peacekeeping operations (contrary to what some may consider revolution in military affairs [RMA] thinking)
- Traditional psychological operations or deception operations
- Covert media manipulation
- Clandestine human intelligence operations or overt research operations

Attempts to avoid the enmeshing phenomenon or to protest that private corporations are essentially that, private, and rely on this as a defense is unwise. It may also be futile. In any event, what is also important is the perception of the other entities with which the private corporation may come face to face (such as substate and non-state terrorist groups, the military forces of other nation-states, and corporate competitors).

Defensive Tactics to Thwart the Threat of Business Spies

Threats to the security of business information are numerous and they come from all directions, including organized crime syndicates, terrorists, and government-sponsored espionage, and most global high-technology companies have little idea of the array of hostile forces targeted against them. U.S. businesses that are increasingly expanding their operations into foreign lands are finding the situation challenging because the nature of such threats and how to protect against them is not taught in business school.

Some of the threats might be obvious, as well as the strategies that companies can mount against them, but others might not be so cut and dried. In a world in which countries measure themselves in terms of economic might, many intelligence services around the world are shifting their emphasis and targets to business. Government-sponsored intelligence operations against companies seek information about bids on contracts, information that affects the price of commodities, financial data, and banking information.

Furthermore, government intelligence services want technological production and marketing information, and they usually share what they get with their country's companies. To get this sensitive information, government intelligence services use many of the techniques developed during the Cold War. That includes bugging telephones and rifling through papers left in hotel rooms by visiting businessmen and businesswomen. In addition, government intelligence services are known to plant moles in companies and steal or surreptitiously download files from unsecured computers. Several also have highly sophisticated signal intelligence capabilities to intercept even encrypted company communications. Messages that are not encrypted with the latest technology are especially vulnerable. These include telecom and computer communications, including email.

Though the French intelligence service is probably the most egregious offender, it is far from alone. Russia, China, South Korea, India, Pakistan, Germany, Israel, and Argentina all have some type of intelligence-gathering operation for the benefit of companies in their countries, and many more countries are doing the same. The United States, however, is not among them.

No American intelligence agency conducts industrial espionage against foreign companies for the advantage of U.S. companies. What the U.S. intelligence community (CIA, NSA, etc.) does is support the efforts of their own government, and that information is not shared with American companies.

Reports originating in Europe, especially France, that the United States is using signal intelligence capabilities as part of a program called "Echelon" to attack European companies for the economic advantage of U.S. companies is simply not true. Another threat comes from the dozens of intelligence services in developing countries that have profited from the training they received from the Soviet Union, Eastern European countries, and the CIA during the Cold War. The result of this history is that the reservoir of professionally trained intelligence mercenaries is growing.

Other threats include terrorism, organized crime, and inside operations carried out by disgruntled employees and hackers. Some of these groups are looking for the greatest amount of destruction, and an attack on the critical information infrastructure of the United States would satisfy that goal.

Business needs to understand that the criminal and terrorist threat worldwide is changing and is now both more sophisticated and more dangerous than anyone would have thought. Vulnerabilities that all the different types of attackers exploit include open systems, plug-and-play systems, centralized remote maintenance of systems, remote dial-in, and weak encryption. Companies could provide substantial information security protection for relatively low cost.

Companies should review security measures in sensitive areas of their operations such as research and development, talk to traveling executives who carry company laptops about using precautions to prevent theft, and examine communications with overseas facilities with an eye toward installing commercially available encryption that is all but impossible to crack. The new algorithm recently approved by the Department of Commerce, for example, is so strong that it would take an estimated 149 trillion years to unscramble.

Company executives should also limit physical access to sensitive data and programs and regularly change computer passwords. It's all obvious, but every one knows how many companies are lax in their actual implementation.

A basic rule is to take time to identify company-critical information, whether it is technology, a production technique, basic research and development, financial information, or marketing strategy, and take steps to protect it. What is required first is simply awareness by CEOs and boards of directors that there is a threat and then, second, response using a common-sense way to protect themselves. These are measures that make good business sense even if you are not a target of a government intelligence service, a competitor, a criminal organization, a terrorist, or a hacker.

Cybersecurity Progress in the Private Sector

Many companies have made significant progress since 2000 to protect their infrastructures from attack, but others still face an uphill battle. Nevertheless, the government and private firms must work together to bolster cybersecurity.

The banking and energy industries remain ahead of many other sectors in security preparedness. Other sectors, including telecommunications, transportation, and waterways, face difficult challenges stemming from a vast array of factors such as deregulation and market fluctuations.

However, progress hasn't proceeded at the same pace in all sectors. There are some sectors that are ahead of others. Nonetheless, private companies accept the challenge that the government has given them to protect the networks that run their infrastructure.

Obstacles

The information technology (IT) sector has been moving very aggressively. Any perceived slowness is due to a genuine desire by industry to protect proprietary and sensitive information on behalf of their companies, shareholders, and clients.

Corporate concerns regarding shareholder value and increased competition may be getting in the way of security progress at some banks, airlines, and telecommunications companies. Despite the banking industry's perceived success in the area of security, a recent spate of money laundering schemes, including a $5.8 billion scam against Citigroup Inc. and Commercial Bank of San Francisco that lasted 13 years, raises serious questions about the status of security in the industry.

Likewise, the airline and telecommunications sectors have come "under siege" as a result of deregulation and the current climate of mergers and acquisitions. Years of a systematic underinvestment in electric power grid capacity, combined with the effects of wholesale deregulation, have created a potentially perilous security situation.

Security protections against cyberattacks in natural gas and electric industries are being addressed constantly, although the national effort lacks a useful gauge of how much security is enough. If you aren't attacked, it's easy to let the program slip.

SURVIVING OFFENSIVE RUINOUS IW

The principal actors in any cyberterrorist attack on a corporation, and the levels on which the attack may be made have already been discussed. This section deals with surviving offensive ruinous IW by looking at the mechanics of attack and defense.

The U.S. General Accounting Office (GAO) has produced a report on information security and computer attacks at the Department of Defense. It identifies the following means of attack:

Sendmail program: Installation of a malicious code in an email message sent over a network machine. As the sendmail program scans the message for its address, you will execute the attacker's code. Sendmail operates at the system's root level and therefore has all privileges to alter passwords or grant access privileges to an attacker.

Computer-searching programs: Password cracking and theft is much easier with powerful computer-searching programs that can match numbers or alphanumeric passwords to a program in a limited amount of time. The success depends on the power of the attacking computer.

Packet sniffing: An attacker inserts a software program at a remote network or host computer that monitors information packets sent through the system and reconstructs the first 125 keystrokes in the connection. The first 125 keystrokes would normally include a password and any logon and user identification. This could enable the attacker to obtain the password of a legitimate user and gain access to the system.

Access: Attackers who have gained access to a system can damage it from within, steal information, and deny service to authorized users.

Trojan horses: An independent program that when called by an authorized user performs a useful function but also performs unauthorized functions, which may usurp the user's privileges.

Logic bomb: An unauthorized code that creates havoc when a particular event occurs (for example, the dismissal of an employee).

It is becoming increasingly difficult for "low-knowledge" attackers to use relatively cheap, "high-sophistication" attack tools to gain access to what was, historically, a relatively impregnable system. The addition to this ready availability of high-technology attack tools of an increasingly networked global economy, and the integration of corporations within that networked global economy, expedientially increases the risk of attack and the ability of any attacker to cause damage.

Surviving a Misbehaving Enemy

Article 99 of the Uniform Code of Military Justice defines misbehavior in the face of the enemy as any person who, before or in the presence of the enemy:

- Runs away
- Shamefully abandons, surrenders, or delivers up any command, unit, place, or military property that it is his or her duty to defend
- Through disobedience, neglect, or intentional misconduct endangers the safety of any such command, unit, place, or military property
- Casts away his arms or ammunition
- Is guilty of cowardly conduct
- Quits his place of duty to plunder or pillage

- Causes false alarms in any command, unit, or place under control of the armed forces
- Willfully fails to do his utmost to encounter, engage, capture, or destroy any enemy troops, combatants, vessels, aircraft, or other thing, which it is his or her duty to encounter, engage, capture, or destroy
- Does not affect all practical relief and assistance to any troops, combatants, vessels, or aircraft of the armed forces belonging to the United States or their allies when engaged in battle
- Shall be punished by death or such punishment, as a court-martial shall direct

Now, you're wondering what this has to do with network security, IW, or yourself—because you are not at war. Let me assure you that it does apply to network security, IW, and to you—and you most certainly are at war.

Every day, someone from a subculture other than your own is waging a battle against you and your systems. As network professionals, you are the propagators of your own doom. You are guilty of misbehavior in front of the enemy by not admitting your own fallibility, by not passing critical information to your own team, and from your sheer arrogance in thinking that you can't be bested by some punk kid.

Remember: misbehavior in the face of the enemy. True, it is not life or death, and hacked systems aren't really your enemy, but the concept is the same. In neglecting to raise the alarm and warn the others, you are guilty of this cowardly act. Open communication is your enemy's greatest advantage and your greatest weakness.

SURVIVING OFFENSIVE CONTAINMENT IW

Using layered biometric tools to boost security is now part of the latest arsenal and tactics private companies use against offensive containment IW. In the race to improve security infrastructures faster than hackers can invent methods to penetrate firewalls [1], it is important to ascertain a user's identity before permitting access to protected data. Given the pervasive use of passwords and personal identification number codes for user authentication across all aspects of our daily life, attackers have developed powerful password-cracking tools.

New technologies that aim to directly strengthen user authentication include the use of tokens and smart cards combined with digital certificates. The most compelling and intriguing authentication technologies involve biometrics matching the measurement of physical and behavioral characteristics such as facial structures, voice patterns, and fingerprints.

Recently, biometrics technology has rapidly pushed through barriers that have slowed its adoption in mainstream environments. Performance, accuracy, and reliability have increased among all types of biometrics methods, and prices for capture devices have plunged, making biometrics an attractive addition to security systems. The remaining challenge for biometrics is to address the requirements for large-scale deployments in complex governmental, institutional, and commercial systems.

To gain widespread acceptance in businesses, multiple individual biometrics methods must coexist in a single-system solution, and the underlying architecture must better support the conditions of interoperability, scalability, and adaptability that govern the total cost of ownership calculations. A multitiered authentication system built around these notions is one solution.

At the center of the authentication system, a server orchestrates interaction among client devices, an authentication validation policy system, multiple authentication matching engines, and databases housing user information. Applications and transaction systems request a centralized authentication server to confirm or deny a user's identity. The server receives incoming requests for authentication and directs actions to gather appropriate user credentials and evaluate them against a set of validation criteria.

The policy system might maintain extensive rules to meet security requirements that may differ depending on the user, application, or transaction task. The authentication security policy may require many biometrics for validation. Thus, the validation system must be able to layer biometrics approaches, balance matching scores from each matching process, and interpret these results in light of preset policies. This process is computationally expensive. It's critical that companies scale with system demand. Because each biometrics method requires a different matching-process engine, the authentication system should distribute the matching task to the correct algorithm and thread the processes across a farm of processors.

The user-interaction tier collects credentials from live users in real time. To collect a new biometric sample, a prompting system must request a specific user action, such as presenting a particular finger for scanning or repeating a voice phrase in a microphone. Many types of point-of-service access devices, such as desktops and laptop computers, mobile phones [2], wireless pocket devices [3], and airport kiosks, may be used at any time by end users. Each device may have limited capabilities to request and gather a specific biometric from the user. Therefore, the authentication server must dynamically determine what biometric to request, based on the client device.

To complete the process, a user's credentials must be evaluated against a stored pre-enrolled user information profile, such as biometrics templates, digital certificate keys, and text passwords. Repositories of this information may be centralized in protected databases or decentralized within personal tokens or smart cards. With the use of a smart card that contains the enrollment data, the authentication server would also prompt users to present their template cards instead of accessing them from a central database.

Although there are advantages to using biometrics, authentication should not forego other methods as part of the overall authentication solution. Even old-fashioned PIN codes and passwords provide an extra layer of protection and may be preferable in lower-risk security systems. Other security technologies, such as public key infrastructure, also perform critical roles in an overall security model.

PARTICIPATING IN DEFENSIVE PREVENTIVE IW PLANNING

An attack on any one of several highly interdependent networks can cause collateral damage to other networks and the systems they connect. Some forms of disruption will lead merely to nuisance and economic loss, but other forms will jeopardize lives. One need only note the dependence of hospitals, air-traffic-control systems, and the food-processing industry on computer controls to appreciate the point.

Stopping DoS Attacks Together

The most recent round of denial-of-service (DoS) attacks shows that cyberterrorism is alive and well, and that e-businesses and their service providers aren't doing enough to stop it. Unfortunately, all corporate America and Internet service providers (ISPs) seem to be focused on is who to blame. After the recent attack on Microsoft shut off access to everything from Expedia to Hotmail, the company attributed the problem to one employee's misconfiguration of a router, yet experts noted that a failure to distribute domain name service (DNS) servers made the company vulnerable to begin with.

If a private company is going to minimize the number and effect of DoS attacks, what's required is a spirit of cooperation between companies and their ISPs, as well as among the ISPs themselves. ISPs are starting to tackle the subject of network-wide security, but they're doing it by laying out requirements for their corporate customers. In many cases, customers either follow the ISP's security guidelines or find themselves a new ISP; there's no room for negotiation. It's high time ISPs and their clients started sharing information about what works (and doesn't work) in terms of network architecture, data access, and security systems.

ISPs must ask themselves whether they're doing everything possible from a network monitoring and warning perspective. They should give serious thought to the latest security tools that can stop DoS attacks at their routers. After all, once an attack gets through the ISP, it's a lot tougher for an individual site to fend it off.

Everyone along the e-business food chain has something to lose when a DoS attack succeeds. The site that's been hit loses traffic, revenue, and customer loyalty. The ISP loses customer confidence and significant resources in combating the attack. Ultimately, every site that relies on the ISP must spend time and resources rethinking its security levels.

ISPs must communicate the types of attacks they're experiencing. They also must be prepared to notify one another of attacks and even coordinate their responses when they do get hit. With so much at risk, it's hard to imagine why these conversations haven't been taking place all along.

Approaching IW Planning with IW Games

It's Independence Day 2006. Glitches in air-traffic-controller screens cause a deadly mid-air collision above Chicago's O'Hare Airport, killing over 456 people in both planes, and over 1,500 people on the ground when the planes plunge into a nearby crowded shopping center. Five weeks later, the company that controls California's power grid somehow misplaces an electrical energy order to Northern California's electric company, leaving three-fourths of Sacramento in the dark. Then in October, a high-power microwave burst fries the electronics at an ebola virus lab research building at Fort Deterick (Frederick, Maryland).

Hypothetical IW planning exercises like these are being played out around the country in preparation for what politicians, the military, and law enforcement officials fear will be an orchestrated cyberattack on critical U.S. private infrastructure companies (see sidebar, "Five Easy Steps to Planning and Launching a Cyberattack"). The theory goes that if a well-funded, organized series of cyberattacks were to strike at a target's economic and structural nerve centers, it would send the target society into chaos and make it difficult for the military to communicate and move troops.

FIVE EASY STEPS TO PLANNING AND LAUNCHING A CYBERATTACK

Here's how a computer invader plans and launches an attack on information systems:

Recon: Invader uses information-gathering programs and techniques to sniff traffic at the network gateway, then scans ports or vulnerable services.

Profile target: Invader gets passwords, then identifies machines and software running on the network.

Attack: Invader gains root or administrative privilege of unclassified systems, then seeks and modifies information.

Cover tracks: Invader hides the evidence trail and slips away.

Wait for results: Invader watches CNN to see what damage he or she wrought.

→

The weak areas are in predicting when someone is gathering information for a later attack, and once a company has been attacked, the problem is in recovery.

Researchers are working on ways to tie an algorithm into other technologies also being researched, including advanced forensics and a tracking system to follow a live evidence trail. Don't be surprised if algorithms eventually wind up in the private sector.

This particular information war game was played out among 119 IT executives attending an IW workshop at NSA Headquarters in Fort Meade, Maryland. In the worst-case scenario, every major industry sector would be affected.

NOTE

Most of the targets in the NSA IW games are private-sector companies.

When you're talking about IW, you're talking about IT systems used to cripple the government and economy. Close to 95% of those critical infrastructure companies are privately owned and operated.

Since 1999, IW preparedness has moved forward the fastest in the highly regulated and well-organized financial, energy, and telecommunications sectors, but IT leaders in the private sector say they're hesitant to report incidents to agencies such as the NSA and the FBI. Still, the agencies need this information for intelligence and predictive analysis.

Although the impact of IW bears the same uncertainty as Y2k did, many IW experts say cyberterrorism and cyberwarfare are inevitable. In 2000, hacking hobbyists showed how easy it is to propagate viruses throughout Internet-connected mail systems. They've also shown they can hack armies of unwitting computers and make those computers do their bidding. Now, the U.S. government is thinking about what terrorists with more resources could accomplish. So are countries such as China and Russia, which are developing their own IW capabilities.

In spite of these indicators, IW thinkers say a cyberwar is years away. Clearly, the eventuality of such an attack is present. That's what motivated the Bush administration to move forward with a national plan, but it's doubtful that anyone has the cyber capability today to launch an attack that would cripple the nation's infrastructure. The presidential directive predicts that such a scenario is still years away.

BENEFITING FROM AND SURVIVING DEFENSIVE RUINOUS IW

Users are drowning in computer passwords. Let's count them for a typical worker. At the office he needs one to log-on to his computer. He needs still another to access his corporate email. He also need three for separate databases within his company:

one for a legal research database (a corporate lawyer), and two to get information on his retirement plan and benefits. When he gets home, he needs a password to log on to his home computer and a handful more to use online services. Amazon.com and other online merchants also require a password to make purchases. To get cash from an ATM, he needs his PIN number.

With as unique a fingerprint as a password, corporations can be sure that a person logging on to a computer network is who he or she claims to be. As previously discussed in this chapter, you can benefit from and survive defensive ruinous IW by using biometric technology (which uses unique human characteristics such as fingerprint, voice, face, or iris patterns to verify a person's identity), which is making rapid inroads into corporate America. According to Gartner Group, within three or four years about 88% of all corporations will use fingerprint readers or some other kind of biometric device.

The scramble to commercialize biometrics stems primarily from changes in how companies organize their information technology. The 1990s switch to network computing, which moved important data from mainframe computers to servers, increased the flow of information within a company, but in the process, it made that information more vulnerable to theft and tampering. A recent FBI survey found that system penetration by corporate outsiders and unauthorized access by corporate insiders are both on the rise.

Corporate networks are not the only potential commercial application for biometrics. Credit card issuers want to reduce losses from fraud. In recent small tests, MasterCard began using fingerprints as a substitute for a signature. Biometrics holds the ultimate security key to future payment systems. The explosion of e-commerce [4] has also created a gigantic need to authenticate the identity of buyers.

The price of biometric devices has plummeted. In 1994, the smallest fingerprint reader sold by Identicator Technology was the size of a telephone and cost $2,000; today it's the size of a sugar cube and sells for $64. In five years, a similar fingerprint reader may cost $10.

It's likely that more than one biometric technology will emerge. Fingerprinting will snag the lion's share in the fast-growing corporate computer network market, but technology using voice identification can be easily integrated into already existing telephone services such as automated call centers that answer queries about credit cards, bank accounts, and benefits. Facial recognition technology also has its advantages.

The ultimate goal for biometrics manufacturers is to get into the homes of millions of consumers, with the PC being the likely point of entry. About 11% of all new PCs, including some laptops, are already equipped with cameras, suggesting that facial recognition may eventually play a role on the Web.

Privacy concerns are a big hurdle. Consumers may decide that using a face or a fingerprint as a password will jeopardize privacy more than protect it.

BENEFITING FROM AND SURVIVING DEFENSIVE RESPONSIVE CONTAINMENT IW

In 2000, hackers launched the now-famous DoS attacks that cost high-profile Web sites about $3 billion in revenue. The events during that 48-hour period in February 2000 were especially fearsome to service providers, who found out just how vulnerable they were. As a result, some ISPs have begun issuing ultimatums to corporate customers: Meet certain security standards or take your business elsewhere.

To be sure, most service providers have not created a formal list of security requirements, but many have some kind of policy that dictates what companies can and cannot do as customers and the kinds of security systems that must be in place before they can purchase services.

These service providers want to see IT managers install encryption and authentication products, firewalls that interact with intrusion detection software, dedicated servers, and virtual private network (VPN) links to secure data. They also want IT shops to use tools such as anti-virus software, specified intrusion detection systems, and anti-spam content filtering. All these security installations are being implemented with the hope that private companies will benefit from and survive defensive responsive containment IW.

Precisely when ISPs started getting tougher is hard to determine, but it's clear that ISPs weren't making these types of security demands before the DoS attacks began. The attacks made service providers aware that it's not just corporate customers getting hacked. The ISPs' systems were commandeered and used to launch virus attacks and DoS attacks, as well as to commit vandalism and theft. That's why some of the most common requirements of the ISPs have to do with customers' outgoing traffic—which can directly affect the ISPs. From the ISPs' point of view, their own customers or prospective customers are now security threats. This new approach by ISPs is being felt by IT shops.

Now, all architecture has to be approved by the security desk before services are offered, and a customer with single-tier access won't be approved, even though many want to be. They have to lease a site-to-site VPN or a dedicated T1 link. The VPN (the cheaper of the two options) costs an additional $790 per month.

The ISP demands don't always result in higher costs for corporate customers because of their financial status in the corporate community. Sometimes providers want to look under the hood.

ISPs' fears may be justified. According to a survey in 2004 by the Computer Securities Institute (CSI) and the San Francisco FBI Computer Intrusion Squad, 83% of CSI's 929 member companies detected unauthorized use of their systems during the previous year, up from 106% in 2003. The rate of hacking is growing faster than e-commerce itself. CSI has 973 security professionals onboard (more than one IT person per company in some cases), and 95% consider disgruntled employees to be the biggest security threat.

Insiders, many service providers agree, are the ones who send spam and launch viruses and DoS attacks. The FBI reports that there are now 500,000 known computer viruses, and that at least 73% of American companies reported that they have been plagued by some type of computer virus.

As far as the ISPs are concerned, viruses are among many security problems they face. In the past year, ISPs have set up entire departments devoted to fielding phone calls and handling subpoenas from individuals and companies claiming that ISP customers are spamming, sending viruses, vandalizing Web sites, and launching DoS attacks.

Service providers, in effect, are establishing rules that make it clear that they no longer want to bear the burden of the risks corporate customers are willing to take. They say it's no longer up to clients to determine how risk-free they want to be when it comes to e-commerce. Ultimately, companies that want ISPs to deliver any service at all (even a simple pipe to the Net) will pay more in hard costs, internal policy changes, infrastructure, and business processes.

How much more companies will pay depends on how secure the ISP thinks its customers' network should be, but the ISP is, in many cases, dictating the terms. Whether the customer buys the needed security technology from the ISP or elsewhere, this technology will have to be bought before network services begin. This could mean a huge cash outlay before service even starts.

Fighting Back

IT managers may be told to spend more on security prerequisites, but there's still room for negotiation. This is an emerging trend, not a government regulation, so it's entirely fair for IT managers to bark back, particularly when many ISPs still can't deliver the security services they're asking customers to have up front.

For example, security is something companies must buy from security management companies, not ISPs. If a company must go elsewhere for security, it then begs this question: What level of security does the ISP offer corporate customers? If ISPs demand that customers walk into the relationship with higher levels of security, corporate customers can turn the tables and demand the same of the ISPs. Corporate customers should be encouraged to push back. When an ISP tells you to open up your system so they can look around and see if you meet their standards, tell them you want them to do the same.

The ISPs must either ensure that their security mechanisms will work or be responsible for damages, so ask about their network-monitoring tools and alert mechanisms. Once companies open up the conversation to include both sides, it becomes more of a negotiation and less of an ultimatum.

Before a company gives an ISP access to its entire network for inspection, it should ask the ISP if it's actually going to manage every aspect of the network. If they're not going to manage a certain aspect of your network, like a certain server, then they don't need access.

It may prove to be more trouble for ISPs to deliver security if parts of a potential customer's network are unknown to them, but that's the ISP's problem. Besides, it's the ISP's responsibility to monitor a customer's outgoing traffic, so the ISP already has access to what it needs to know to protect itself. If the ISP's monitoring tools aren't robust enough to give it intelligent reporting, traffic analysis, and alerts to red flags, that's something corporate customers should try to get the ISP to deliver.

The best way to protect the company is to handle these issues in the service level agreement (SLA). The ISPs have the leverage to force customers to implement security, but customers also have a certain leverage. The ISP market is more competitive than ever.

According to Gartner Group, there are now tens of thousands of full-service ISPs, up from less than 1,000 since 1999. The competition means it's in the ISP's best interest to offer corporate customers as much value-added as possible. There's one caveat, however: the idea is to get the ISP to concede some points—for example, help with making the company's network compatible with the ISP's or on-site tech support.

The reality is that even if ISPs can dictate security policies, they will be eager to offer value-added services. If you do the negotiating in the context of drafting an SLA agreement, it shows the ISP you're a serious customer and gives them an opportunity to offer you fee-based services over the long term.

A good SLA won't get the company out of paying more for application service providers (ASP) and ISP services in the end. In fact, it can end up costing more—but it will at least get the company the most bang for the buck. The truth is that ISPs will dictate how much security customers will have because they can. They are the conduits to the networks.

IT managers should understand that pushing back at the ISPs will only do so much. This is a trend that's here to stay. The ISPs started the trend, but it won't end with them. Business partners and regulators will step in and give the security push even more teeth, including standards such as best practices and default security requirements.

Ultimately, the ISPs will protect themselves from outgoing traffic by shutting Web sites down that have been commandeered for DoS and other attacks. The ISPs that survive will start offering security services. It's only during this interim period that the onus will be on companies that use ISPs to pick up the slack. Whether the time period is six months or six years is hardly important. Companies that want to do business with top-tier providers had better get serious about security.

PROTECTION AGAINST RANDOM TERRORIST IW TACTICS

Are ASPs and hosting providers selling customer information? How can private companies protect their data against random terrorist IW tactics? The answer lies between the implementation of data-protection techniques and firewalls—both are briefly covered in this section.

An information security officer for the New York State Office of Mental Health is considering the ASP model, but he's afraid patient data could end up in the wrong hands.

Data security concerns, too, tarnish ASPs' allure for government clients. Think of the commercial windfall if any of these hosting companies started selling social services data or any other government agencies' data. It's unacceptable, but it could happen. And indeed it does.

According to a recent industry survey, 33% of application-hosting providers were selling their customers' data. What is most disturbing is that the hosting companies all had privacy policies in place, which they were violating.

The would-be gatherers of the stolen data aren't always advertising agencies or marketing firms. They could be random terrorists seeking out corporate data (any data) to destroy as part of an IW tactic. For example, one ASP executive reported software vendors asking him to host their applications for vertical market customers so they could mine the customers' databases. At least, that's what they claimed to be doing. The vendors wanted to act as purchasing agents between the members of those vertical markets, enabling them to sift through the members' databases for information to cross-sell between the member companies. If the customers agree, it could be great, but that is a big if. Most companies don't want anyone mining their data.

Selling customer data is taboo for most ASPs, whose executives cringe at the prospect and chalk it up to a few bad apples who will soon be out of business. If it is happening, it could have terrible implications for the rest of the industry, but most ASPs view their customers' data as their sacred asset and would never consider selling it. An ASP should also be bound to a privacy policy as part of the service contract.

Prevent your data from being sold up front by making the ASP sign a contract that says they can't sell it. Make sure you take a close look at the wording to see what constitutes a sale or transfer of data (see sidebar, "Data Protection Measure Tips").

DATA PROTECTION MEASURE TIPS

Application-Hosting Providers

- Consider working with a lawyer or auditing firm when writing a privacy contract.
- Limit staff access to data and set up multiple levels of security.
- Require employees to sign a statement that they will abide by security and privacy policies.
- Separate the data center from corporate offices.
- Have one-door access to the data center.
- Install security cameras in the data center.

Customers

- Examine a privacy policy's wording to understand what constitutes a sale or transfer of data.
- Keep the "what-ifs" in mind: If providers go bust or are acquired, what happens to the data?
- Do a background check on the provider and check references.
- Look for seals of approval.

What if the hosting provider goes out of business? Is it permissible to sell its customers' information as an asset (as online retailer Toysmart.com tried before being rebuffed by the Federal Trade Commission)? What if the ASP is acquired? Will the acquirer stick to the same privacy agreement (see sidebar, "Privacy Agreements")? An ASP should be able to answer all these questions.

PRIVACY AGREEMENTS

What's stopping hosting providers from selling their customers' data? Ethics and little else, according to industry watchdogs. Companies are tempted to sell valuable information at their disposal because there are no set legal ramifications to doing so. Right now, a lot can be bought and sold rather freely, and that includes the business sector. The pressure right now to sell data applies to business information as well as to consumer data. People tend to overlook that.

→

Hosting providers can be held accountable if they violate their privacy policies, but privacy policies often are more vaporware than reality. Privacy policies have more holes than Swiss cheese.

Customers must take some of the blame for flimsy privacy policies because many only skim over privacy statements in their rush to sign on with an ASP. A lot of ASPs offer free services. They say, "Sign up now and get the first few months free." In their rush to sign on, customers don't even look at the privacy policy.

However, the ASP industry aims to police itself. The ASP Industry Consortium is working with the World Intellectual Property Organization to establish dispute resolution procedures between ASPs and their customers, covering such areas as copyright and proprietary rights infringement and loss of data or data integrity.

Companies hosting data also should take measures to prevent internal and external marauders from gaining access to customer information. Many ASPs, for example, check the backgrounds of the data center staff and restrict their access to data. Often, the customer, not the ASP, chooses who gets access.

Another safeguard is making data center employees pass through several security levels, including physical security guards, key-card door access, and even biometric hand scans. A common mistake made by ASPs is housing the data center in the same facility as a corporate office. For example, it's too easy to say, "I work with the company," flash an ID and walk right in." It's easier to be able to bypass external data center security measures by pretending to be a member of a nightly cleaning crew and telling a security guard that he or she was with a group already in the building.

To test an ASP's privacy policy and security measures, customers should hire an outside auditing firm. Customers should also test an ASPs' security measures up front and use an auditing firm to test them on an ongoing basis. Some ASPs even get in on the auditing act.

Another data safety avenue for ASPs are seals of approval from such organizations as the Better Business Bureau and TrustE. TrustE, of San Jose, California, gives out privacy seals of approval, called "trustmarks," to Web sites. It's also considering expanding the program to include software companies. To get a privacy seal of approval, software companies have to disclose their data-gathering and dissemination practices. That might become more common. ASP clients are sharpening their scrutiny of data privacy. Customers of ASPs are taking a long look at privacy policies. Most won't work with ASPs that don't have a solid one in place.

WHAT TO DO WHEN TERRORISTS KEEP ATTACKING

Today, e-commerce and information sites worldwide remain vulnerable because there are (still) no strong defenses deployed—thus, terrorists keep attacking. Although repeated attacks have increased awareness of the problem, and technologies for dealing with DoS attacks are seemingly on their way, the attacks have become more sophisticated—and the problem is not going away. At least one tester of anti-DoS technology (a major Internet provider) has estimated that anywhere from 9 to 14% of the traffic on its networks is, in reality, data sent by vandals intent on a DoS attack.

The attacks have gone from just Web servers to enterprises and infrastructure. Private companies cannot become complacent. So, what do you do when terrorists keep attacking?

Solutions on the Way

Several groups are attempting to work together to fight DoS attacks. The Internet Engineering Task Force has started working on a technology to trace the origin of a piece of data back to its source. So-called ICMP Traceback Messages, or itrace, could turn DoS attackers from anonymous vandals into easily tracked criminals. Other groups are forming to share information about attacks, to be better prepared to defend against them.

The Information Technology Association of America, with 23 other major technology companies, has formed the Information Technology Information Sharing and Analysis Center, or IT-ISAC. By sharing attack data, members are better prepared for future DoS attacks (among other Internet threats) and are better able to track attacks to the source.

Such tracking is difficult today because the tools used by the vandals who start such attacks can be modified to appear to come from a completely different source than the real one. Called "IP spoofing," such a technique requires every company whose server routes data to cooperate to pinpoint the attacker. Without such cooperation, an attacker may be difficult to find, but stopping the attack is possible. The Holy Grail is to have a ubiquitous deployment all throughout the Internet.

Today, customers are more interested in keeping their connection to the Internet up and working than prosecuting an attacker. The customers' first priority is not to make these things go away. They just want to keep on doing business.

Everyone Must Work Together

While some companies want just to keep on doing business and not solve the computer attacker prosecution problem, others believe the problem won't be solved without Internet-wide cooperation. The only solution is to trace things back and turn them off, and that requires a lot of cooperation. Any technology like these has to be widely deployed. It has got to be a community effort.

DoS attacks seem to (and in some cases, actually do) come from dozens or hundreds of locations at the same time. Without Internet service providers cooperating, tracking the attacks is impossible. Cooperation has become critical because the Internet is still rapidly growing, and more, rather than fewer, mistakes are being made. There are more and more machines out there, and consequently, that means more and more vulnerable machines. The attacks on Microsoft have shown that hackers are more than willing and able to carry out successful attacks. Until companies act together to make the Internet more reliable, business on the Net is at risk.

Hack Back

"Hacking back" is another tactic that private companies can use when terrorists keep attacking. However, some companies have become either virtual vigilantes or packet pacifists. Network executives have mixed feelings about whether to retaliate against an attack.

In December 1999, when protesters were rampaging through Seattle in an attempt to disrupt the World Trade Organization (WTO) summit meeting, other activists were launching a DoS attack on the WTO Web site. The WTO's Web-hosting service spotted the attack and repelled it, bouncing the flood of page download requests back to the origin server, which was run by a group calling itself "electrohippies." The e-hippies coalition, based in the U.K., never publicly acknowledged that the attack had been turned back on its own server, but the next day, a notice appeared on the e-hippies site apologizing for people having problems getting through to its site.

To retaliate or not to retaliate? In cyberspace, there is no simple answer.

Conxion, the San Jose hosting service that reversed the attack on the WTO server, recognized the attack was coming from a single IP address belonging to the e-hippies server. Conxion then redirected their filtering software to redirect any packets coming from these machines back at the e-hippies Web server. Conxion was so proud of having given the attackers a dose of their own medicine that it issued a press release about the incident. However, the reaction among IT professionals to the counterstrike was decidedly mixed.

According to industry analysts, most IT professionals will not strike back in cyberspace, for fear of hitting an innocent bystander, but they're not averse to taking some action when they're sure of the perpetrator's identity.

If vendor tools are any indication, fighting back may indeed be gathering acceptance in the IT community. Intrusion detection tools, for example, can be configured to reverse attacks. New reactive tools are also popping up in the marketplace, and freeware attack-reversing tools abound on the Web. Nevertheless, brace your networks for more distributed attacks, nastier viruses, and more chaos until these issues sort themselves out. Cyber crime is going to get worse before it gets better.

COUNTERING SUSTAINED ROGUE IW

Corporate reputations have taken a sustained beating from rogue Internet messages, fake press releases, and "gripe sites." Of course, critical opinions are legally protected as free speech, but when the messages are false, defamatory, or designed to manipulate stock values, corporate America fights back.

To do that, companies are hiring Internet IW monitoring firms that use software that scans the Internet to find out what's being said about business clients. They're also hiring private investigators to track the perpetrators, but that's not something you want to do if you're merely aggravated about the messages, because the investigation can be very expensive—for example, $70,000 to $80,000.

The investigations usually turn up former employees, disgruntled insiders, or stock manipulators. The big challenge is identifying the people behind the anonymous screen names. A flurry of messages may actually be the work of only one or two people who use different handles to make it look like they're a crowd.

One approach is to file a "John Doe" lawsuit and use subpoena power to obtain the identity of the mischief maker from his or her Internet service provider. It should be a serious lawsuit, based on a cost-benefit analysis.

Another technique employs "forensic psycholinguists" (the same folks who analyze hate mail sent to the White House), who look for signs that the messages came from the same poison keyboard. In one recent case, a psycholinguist studied 40 messages from three screen names and concluded that they came from the same writer because they had the same format: a question in the headline and the answer in the body. The messages also used the same vulgarities.

Based on the analysis, the psycholinguist surmised that the writer was probably 40, white, professional, and perhaps a day trader. Furthermore, the analysis indicated that he or she suffered from low self-esteem and felt his or her regular job was threatened by the acquisitions of the company he or she was berating.

Private eyes can also engage suspects in online conversations to seek clues about their identities, but there's a danger that the undercover gumshoe could tip his or her hand or cross the line into entrapment. There are even better investigation tricks. For example, perpetrators may have left some electronic footprints behind by filling out a Web site guest book with the same cybersignature they use later for derogatory messages.

Sometimes the text of a message itself provides clues. If they say it's snowing outside, you can check weather records to find out where on the planet it's snowing right now, to narrow the suspect pool. If they say they have a blue

Jaguar and live in Ohio, you can get a database that lists every blue Jaguar owner in the state.

Apparently, private companies are willing to go to great lengths to identify Internet content that besmirches their corporate reputation or infringes on their intellectual property, but such services can be used for much more than just defending against sustained rogue IW in the form of defamation and piracy. Clients start off having a defensive mindset, but then they transition to more of an offensive approach.

In other words, they begin to use Internet surveillance for benchmarking and competitive intelligence, such as finding out when a competitor adds a new feature, such as online customer chat, to its Web site. Internet surveillance can even help companies gather soft information such as “marketing buzz” from the world’s largest focus group.

Law enforcement’s new weapons for protection against random rogue IW, with regard to electronic detection, have spurred privacy proponents to strike back, but will these shifting tactics by law enforcement agencies really protect private companies?

PROTECTION AGAINST RANDOM ROGUE IW

The growing availability of powerful encryption has, in effect, rewritten the rule book for creating, storing, and transmitting computer data [5]. People everywhere rightly regard confidentiality as essential for conducting business, protecting against random rogue IW, and ensuring personal privacy [6]. Governments worldwide have been sent into a spin for fear secret encryption keys will add to the weapons of terrorists and other criminals. Some nations have even attempted to control the technology by constructing a maze of regulations and laws aimed at blocking the import, export, or use of encryption software. Such bans have largely failed.

Recently, the war over encryption has moved beyond controlling the technology itself. Now, some governments are granting law enforcement agencies new powers and funding the development of new tools to get at computerized data, encrypted or otherwise. Rising to that challenge, privacy proponents are striking back with new techniques for hiding data and preserving anonymity in electronic communications.

New Legislation

One legal tactic being used by states is to require owners of encrypted files to decrypt them when asked to by authorities. So far, only Singapore and Malaysia have enacted such laws, with Britain and India about to follow suit.

In Britain, two recent bills would give law enforcement officers the authority to compel individuals to decrypt an encrypted file in their possession under pain of a two-year jail term. Further, anyone given such a command would have to keep the giving of the notice, its contents, and the things done in pursuance of it secret—on penalty of a six-year jail term. The bills broadly define encryption, even including what some consider to be mere data protocol.

Straightforward though it seems, the approach is technically flawed. After all, a suspect may truly be unable to decrypt an encrypted file. He or she may have forgotten or lost the key. If public-key encryption was used, the sender of a file will have the key used to encrypt the file, but rarely, if ever, the decryption key, which remains the exclusive property of the intended recipient. If symmetric key encryption was used, and the sender's hard disk crashes, the key will likely be wiped out along with all the other stored data. This flaw in the legislation was demonstrated by a British group that mailed an ostensibly incriminating document to a government official and then destroyed the decryption key, making it impossible for that official to decode the file, even if "compelled."

Moreover, according to the latest version of the Cyberspace Electronic Security Act (CESA), police would be at liberty to present a text in court and claim it was the decrypted version of an encrypted file, without revealing to the defendant exactly how they arrived at the plaintext. This means the defendant may have a hard time defending himself and makes it a lot easier for the police to fabricate evidence. The ability to receive a fair trial could be at stake.

Escrowed Encryption

Another controversial scheme for letting law enforcement in on encrypted data is known as escrowed encryption. Here, a third party is appointed by the state to keep a copy of the decryption keys (in escrow, as it were) for the state to use to decrypt any file sent to or by any user. In other words, encrypted files would be protected—except from the state.

Needless to say, many people abhor the mere idea. Even if a sound case could be made for revealing the decryption key to government personnel, what is to prevent them from reusing that key in the future to look at other documents by the same user? Furthermore, drug traffickers, terrorists, and others of most concern to law enforcement are the least likely to use encryption that is openly advertised as readable by the government.

Then, too, given the transnational nature of the Internet, a global key-escrow system would need to be established. Sovereign states, with their own interests to protect, would object to such a system; this happened with the escrow scheme known as the "Clipper Chip," which was heavily promoted by the U.S. government but largely dismissed by other states. The logistics of who keeps the escrowed keys, who has authority to demand their release, under what conditions, and so on, becomes unwieldy when vast numbers of encryption keys, states, and legal systems are involved. In view of such concerns, official support for escrowed encryption has all but died in the United States and elsewhere.

Global Surveillance

The ineffectiveness of legal constraints on encryption appears to have persuaded many governments to change direction. They are instead seeking to capitalize on the unencrypted nature of most digital traffic and to derive information by monitoring that traffic. Even encrypted messages tend to leave unencrypted who is communicating with whom and when.

Officially, most states deny the existence of electronic surveillance networks, but extensive claims of their existence persist. Echelon and the Federal Intrusion Detection Network (FIDNet) are two such alleged intelligence-gathering efforts that have been frequently described in the mainstream press and debated in official hearings by government legislatures. Echelon is, according to the Washington, DC–based Federation of American Scientists, a global network that searches through millions of interceptions for preprogrammed keywords on fax, telex, and email messages.

The same sort of public inquiries have been made about the Federal Intrusion Detection Network (FIDNet) that the U.S. National Security Council has proposed creating. It would monitor traffic on both government and commercial networks, with the stated goal of safeguarding the critical U.S. information infrastructure. Although the House Appropriations Committee did away with funding for it last summer, FIDNet supporters continue to push the program, arguing that it would not intrude on individuals' communications. Meanwhile, a number of civil rights groups, including the Electronic Privacy Information Center (EPIC), in Washington, DC, and the American Civil Liberties Union, based in New York City, have challenged FIDNet's constitutionality. The plan demonstrates that privacy concerns are being swept under the carpet.

Computer Forensics

As society relies increasingly on computers, the amount of crime perpetrated with the machines has risen in kind. To law enforcement's delight, electronic records have proved to be a fertile ground for detectives. Indeed, in their present shape, computers, the Internet, and email are the most surveillance-friendly media ever devised.

This development has given rise to an entirely new industry: computer forensics. Its purpose is not only to find out what files are stored in a computer, but also to recover files that were created with, stored in, sent by, received from, or merely seen by that computer in the past, even if such files were subsequently "deleted" by the user.

The ability to resurrect electronic paper trails from supposedly deleted files stems, in large part, from the features built into many computer programs. For example, the delete command in most software does not delete. It merely marks the space that such a file occupied in a disk as being available in the future to be overwritten.

If it was really deleted, then undelete commands would not work.

Also, many Windows applications save temporary versions of a file being worked on, just in case the computer crashes. Even if a user were to deliberately overwrite the original file, the temporary version still lurks in some part of the disk, often with an unrecognizable name and occasionally even invisible from the conventional directory.

Electronic paper trails are also left behind by the fast save function, which saves the latest version of a word-processing document as the original plus the sequence of changes made to it. A recipient of the electronic end result can see how the document evolved over time—not the kind of information most people care to share.

Internet-related applications, like many other software programs, do a lot of internal housekeeping that involves writing information onto the hard disk. For example, the popular Web browser Netscape Navigator creates a file called netscape.hst, which gives a chronological listing of almost everything its user has done with the browser since it was installed.

Simply surfing the Web pushes other data into computer memory, in the guise of "cookies" and as documents "cached" on one's disk. Web sites visited can learn the visitor's Internet service provider, Web browser, and a lot more. A remote Web site could even gain full access to a visitor's hard disk, depending on how aggressive that remote site elects to be and how extensive the protective measures taken by the visitor are.

Software tools now make it fairly straightforward to get a computer to cough up information that its owner may not realize is there. Not to be outdone, computer programmers have developed numerous tools that can defeat most computer forensics tools. Although such counterforensics programs will remove most traces of sensitive data from a computer, it is extremely difficult to remove all traces that may have been left behind. In the absence of a thorough schooling in the esoteric details of computers, the odds favor the competent computer forensics investigator.

Also favoring the forensics expert are new laws legalizing the accessing of computers by law enforcement agencies. In December 1999, for example, the Australian Parliament passed a bill giving the Australian Security Organization the power to obtain warrants to access computers and telecommunications services and, if necessary, to delete or alter other data in the target computer and conceal the fact that anything had been done under the warrant. As of February 2000, Dutch authorities are permitted to use bugging devices in computers to retrieve text.

Countermeasures

The various legal roadblocks and technical wizardry contrived by governments and law enforcement to block encryption's spread have, of course, curbed neither the need for the technology nor the ingenuity of privacy-loving programmers. As a result, a number of countermeasures have been engineered to augment or replace encryption. Among them are anonymizers, which conceal the identity of the person sending or receiving information, and steganography, which hides the information.

The need for anonymity in a democratic society has long been recognized, to shield whistleblowers and political dissenters from retaliation, to protect the records of medical patients, and so on. Less dramatic situations also justify anonymity, such as placing a personal ad or seeking employment through the Internet without jeopardizing one's current job. To be sure, anonymity can be exploited by sociopaths seeking to avoid accountability for their actions, but, in general, it serves a useful social function.

Anonymous and pseudonymous remailers are computers that are accessible through the Internet that launder the true identity of an email sender. Most are operated at no cost to the user. A pseudonymous remailer replaces the sender's email address with a false one and forwards the message to the intended recipient. The recipient can reply to the sender's pseudonymous address, which, in turn, forwards the response to the sender's true address.

Anonymous remailers come in three flavors: cypherpunk, mixmaster, and Web-based. Cypherpunk remailers strip away the message header, which describes where the message came from and how it got there, before forwarding the message to the recipient. Conceivably, someone with physical access to such a remailer's phone lines could correlate the incoming and outgoing traffic and make connections.

Mixmaster remailers avoid that problem by using stronger encryption and tricks for frustrating traffic analysis, such as padding messages to disguise their true length. But even mixmasters can be compromised. For example, through a concerted effort, it would be possible to detect a correlation between Mr. A sending an encrypted message through a remailer, and Ms. B receiving a message at some variable time afterwards.

Web-based anonymizers range from sites offering conventional anonymizer services to others where the connection between the user's computer and the anonymizer is itself encrypted with up to 128-bit encryption. The job is done using the standard secure socket layer (SSL) encryption built into all Web browsers of recent vintage.

For extra privacy, a message may be routed through a series of remailers. For example, the Onion Router project (see the site at *http://www.onion-router.net*) of the Naval Research Laboratory in Washington, DC, offers another way to string together remailers. What's more, it allows anonymized and multiply encrypted Web browsing in real time.

Onion routing is a two-stage process. The initiator instructs router W (in this case, a proxy server at the firewall of a secure site) to create an onion, which consists of public-key-encrypted layers of instructions. Router X peels off the first layer of the onion, which indicates the next step in the path and supplies a symmetric decrypting key for use when the actual message comes through later. The onion then goes to Routers Y and Z, depositing keys at each stop. Once the connection is established, the encrypted message is sent through and successively decrypted, arriving at the recipient as plaintext. To respond, the recipient sends the message to Router Z, which encrypts the text, onion-style, and sends it back through the already established path.

Hiding Data

The microdot used by German spies during World War II to transmit strategic information is an example of steganography, used to hide data in plain view. The microdot consisted of a greatly reduced photograph of a page of text, which was pasted over a period in an otherwise innocuous document. A more modern application is the digital watermark, used for identifying official copies of copyrighted images and recordings. Unlike encryption, which hides the content of a message in an obvious manner, steganography hides the mere existence of anything hidden. The commercially available computer-based steganography programs popular today rely on three techniques:

- Merging the information to be hidden into a "cover" sound file by changing the least significant bit of each digitized sample of the file. The resulting file sounds the same to the human ear and is the same length as the original file.
- Merging the information to be hidden into a cover image file by changing the least significant bit of the digitized value of the brightness of each pixel. Typical images use 256 levels of brightness, with 8 bits per pixel for black-and-white images and 8 bits for each of the three primary colors (red, green, and blue) per pixel for color images. A lot of data can lurk in a 1024 × 768-pixel image.
- Hiding data in the areas of a computer floppy disk or hard drive that are normally not accessed. A computer disk is divided into clusters, each of which holds from 512 to over 32,000 bytes. When a file is saved, it uses a portion of one or more clusters; because DOS and Windows store only one file per cluster, the space left over between the end of a file and the end of the cluster (called the slack) is available to hide data in. This scheme is extremely easy to detect, however.

The Future of Encryption

Encryption today is as strong as it is because there is no need for it to be any stronger. Of course, the underlying mathematical assumptions might be challenged by a breakthrough, such as a solution to factoring large numbers into their prime-number components. Meanwhile, an encryption method can be strengthened by merely adding bits to the encryption key.

Nevertheless, several schemes under development may eventually find use for electronic communication and storage: elliptic curve encryption, voice encryption (already freely available and used worldwide over the Internet), quantum cryptography, and DNA cryptography.

Few microprocessors have been specially designed to run encryption software. Most personal computers can accommodate the hardware and software requirements of modern encryption, but most hand-held devices cannot. For these devices, a new class of algorithms, known as elliptic curve encryption, is claimed to provide encryption strength equal to that of the standard algorithms in use today, while using a smaller key and arithmetic that is easier on microprocessors and that needs much less memory. Being a new type of encryption, its security has yet to withstand the concerted scrutiny of experts.

Voice encryption is a response to the increasing flow of audio traffic over the World Wide Web, which has led, among other things, to the merging of strong encryption with Internet telephony. Given appropriate software, anyone today can carry on fully encrypted conversations with any other user connected to the Internet.

Perhaps the most advanced such software is Speak Freely, which is available worldwide free of charge (see *http://www.speakfreely.org*). Some mainstream voice-over-the-Internet services do not offer encryption, though. Instead, they route the data through the company's servers, thereby opening up a security weakness.

Quantum cryptography is not in itself an encryption algorithm. Rather, it is a means for creating and securing the distribution of private keys. Based on the Heisenberg uncertainty principle, the idea is that communicating photons cannot be diverted from the intended recipient to the unsought-for interceptor without creating an irreversible change in the quantum states of the system.

The precepts of quantum cryptography date from the early 1970s, and research has been ongoing for the past decade at universities such as Johns Hopkins University, in Baltimore, Maryland, and the University of Geneva in Switzerland; at U.S. national laboratories such as Los Alamos; and in the corporate sector, at British Telecom and elsewhere.

In DNA cryptography, each letter of the alphabet is converted into a different combination of the four bases that make up human deoxyribonucleic acid (DNA). A piece of DNA spelling out the message to be encrypted is then synthesized, and the strand is slipped into a normal fragment of human DNA of similar length. The end result is dried out on paper and cut into small dots. As only one DNA strand in about 30 billion will contain the message, the detection of even the existence of the encrypted message is most unlikely.

Shifting Attitudes

If, as seems likely, encryption and related products continue to develop for personal and commercial uses, countries will have to rethink their policies toward the technology. In what may be a sign of things to come, the German government announced in May 1999 that it would fund the development and free distribution of open-source encryption software that the government itself will be unable to break (see *http://www.gnupg.org*). The Federal Ministry of Economics and Technology released a report stating that Germany considers the application of secure encryption to be a crucial requirement for citizens' privacy, the development of electronic commerce, and the protection of business secrets.

Also in 1999, French Prime Minister Lionel Jospin announced a similar shift, saying that his country would scrap any key escrow plans in favor of free use of cryptography. In both cases, the motivation seems to have been the realization that protecting data from foreign parties outweighs any law enforcement concerns, and that the use of strong encryption furthers, rather than hinders, national security.

Independently, the Canadian government announced in October 1999 that it would not seek to regulate the domestic use of encryption. The significance of such trends is clear: the global reach of the Internet has made it extremely easy for encryption software to travel between countries, with or without controls, and if one or more major countries elects not to enforce controls, the technology will spread even more easily. Society's transformation into a computer-based economy makes protecting corporate and personal information not only desirable but also necessary.

How then does one balance privacy and confidentiality with security? Governments are undoubtedly obligated to protect their citizens from terrorism and out-and-out criminality. A partial solution may be to criminalize the use of encryption only in the commission of generally recognized serious crimes and to encourage its use elsewhere.

Attempting to control encryption, however, has proved to be an ineffective means of preventing crime and may actually hurt vital national interests. Similarly, the granting of new policing powers to law enforcement agencies will do less to protect a country's critical infrastructure than building better security technology. If greater security is truly what governments are after, then much can be done with the tools already at hand: encrypting all important data and communications makes their illegal retrieval and interception useless to the thief.

KEEPING THE AMATEUR ROGUE OUT OF THE CYBERHOUSE

Finally, how do you keep amateur rogues out of the cyberhouse? Today, you probably can't, but, tomorrow (see Chapter 17, "The Information Warfare Arsenal of the Future")—well, that's another matter.

Today however, motivated amateur rogue "hacktivists" have grabbed headlines, announcing they've collected credit card and other personal data on some 58,800 business and political leaders. Increasingly, these amateur social activists have turned to hacking to make their point, breaking into computer systems and wreaking havoc on organizations they oppose. The Internet has turned out to be a remarkable tool for nonviolent protest on a scale activists could only dream of before.

The term *hacktivist* was first applied to supporters of the Zapatista rebels in Mexico's southern state of Chiapas, who have sabotaged Mexican government Web sites since 1998 and held "virtual sit-ins" designed to overload servers. More recently, the tactic has been used in Serbia, Pakistan, and India—and by both Palestinians and Israelis in the Middle East. In one case, Palestinian sympathizers broke into a Web site operated by a pro-Israel lobbying group in the United States, stealing credit card information and email addresses.

The theft of private data is a relatively new tactic, which goes beyond defacing Web sites and electronic bombardment of servers. Antiglobalist protesters contend the WTO's trade treaties benefit big corporations and rich countries at the expense of the environment and workers. Protesters who showed up in person were largely stymied by a heavy police presence at the recent Davos meeting. Online, however, they effectively surmounted physical barriers.

Another Frontier

The Net is another frontier for people to engage in these types of activities. The attacks against forum organizers showed just how far hacktivists could reach. They obtained the travel itineraries (including flight numbers) of politicians from around the world and published them on the Web. This poses operational security problems and goes beyond what's been seen before.

Finally, almost every major corporation and organization has been hit at one time or another by hacking, with McDonald's, Starbucks, and the WTO being favorite targets of hacktivists. In some respect, it is really quite clever and quite funny.

SUMMARY

The development of the Internet presents serious threats to the security of private companies, in addition to the much-touted opportunities it provides. The more extreme scenarios discussed in this chapter may never occur. The possibility that they may, however, must be appreciated. It is not advisable for any risk-management approach to disregard the threats previously discussed on the basis that they are far-fetched and fanciful. In addition to the threats being technically feasible, either now or in the next two decades or so, the ability of intruders to gain entry to computer systems and disguise the very fact of entry makes this a peculiarly difficult threat to appreciate. The undetectability of many attacks may lead private companies to a false sense of security and leave the companies vulnerable to serious disruption or total disablement in the event of an attack.

The possibility of means of attack this presents to aggressors can help realistically guide the process of moving forward in dealing with the IW arsenal and tactics of private companies.

Conclusions

- As competition for profit increases between corporations and consumer expectations grow, there may soon be a time that, for some private companies, even a limited disablement may be fatal, or nearly fatal, to its continued existence, surely one of the most important post-threat outcomes of any risk-management plan.
- The growth in the number of aggressors must also be appreciated.
- Added to the traditional aggressors identified by private companies are the ones that may now see the companies as a visible surrogate of an entity that is either impregnable from attack or that it is inadvisable to attack.
- Some private companies have always been the target of aggression, and the identity and number of aggressors may stay the same.
- It must be appreciated that new, and very powerful, tools of aggression may now be available to those traditional aggressors.
- Traditional forms of risk management are, it is argued, not particularly suitable to the dynamic, desegregated forms of aggression.
- The approach to determining risk and how to protect against and prevent network attacks must be revised. A fundamental rethinking of the way private companies organize themselves, and the way they leave themselves at risk, will also be necessary.
- Traditional forms of risk management represent an approach positioned in a hierarchical paradigm, which may not deal adequately or at all with new forms of threat posed to a dynamic network.
- Until these fundamental issues are addressed, no private company can truly say that it has identified all forms of risk that are or will be relevant to that organization. Nor will it be able to say that it has treated them. These must be imperatives in an environment where any single risk could conceivably threaten the entity's survival.

An Agenda for Action

Management of cyberterrorism risk must be considered an important issue for all aspects of society, not only for private companies. However, in view of the way in which the information network has developed, and the almost complete immersion of much of private enterprise in it, a company should analyze its vulnerabilities regardless of societal views.

The dangers in failing to recognize the risk could be serious. The dangers in recognizing the risk but not treating it, could be equally serious.

The U.S. government needs to set an agenda for action that goes beyond the work already done in preparation for protecting the IW arsenal and tactics of private companies. With the preceding in mind, when completing the Information Warfare Arsenal and Tactics of Private Companies Checklist (F16.1 in Appendix F), the computer forensics specialist (CFS) should adhere to the provisional list of actions for networks. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these systems have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? As competition for profit increases between corporations and consumer expectations grow, there may soon be a time when, for some private companies, even a limited disablement may be fatal, or nearly fatal, to its continued existence, surely one of the most important post-threat outcomes of any risk-management plan.
2. True or False? The decrease in the number of aggressors must be appreciated.
3. True or False? Added to the traditional aggressors identified by private companies are the ones that may now see the companies as a visible surrogate of an entity that is either impregnable from attack or that it is inadvisable to attack.
4. True or False? Traditional forms of risk management are particularly suitable to the dynamic, desegregated forms of aggression.
5. True or False? The approach to determining risk and how to protect against and prevent network attacks must be revised.

Multiple Choice

1. Various aspects of society are being transferred to cyberspace, except:
   A. Informational activities
   B. Transactional activities
   C. Architectural activities
   D. Infrastructure activities

2. There are three general categories of attack especially applicable to a private enterprise, except:
   A. Data destruction
   B. Information attacks
   C. Penetration of a system to modify its output
   D. System penetration with the goal of stealing information or sensitive data

3. The collapse of the former Soviet Union into what could be termed a "transnational kleptocracy," has led to some fundamental changes in the international security environment, except:
   A. Small numbers of unemployed, underemployed, or otherwise disaffected security and KGB operators are now available for hire.
   B. Large numbers of highly trained and professional scientists and computer experts may no longer have jobs.
   C. Some countries into which the former Soviet Union disintegrated have a nuclear capability and/or reserves of highly enriched uranium.
   D. Some estimates claim that 73% of the Russian economy is under the control of criminal enterprises. These enterprises have spread beyond the borders of any particular state.
   E. Estimates claim that 89% of Russian banks are under criminal control.

4. The three elements of IPK are, except:
   A. Open source intelligence
   B. Information technology
   C. Electronic security and counterintelligence
   D. Political, ethnic, and religious groups

5. IP is:
   A. Internet protocol
   B. Application of information or information technology in support of conventional military peacekeeping operations (contrary to what some may consider revolution in military affairs [RMA] thinking)

C. Traditional psychological operations or deception operations
D. Covert media manipulation
E. Clandestine human intelligence operations or overt research operations

Exercise

In the preliminary stages of an employment dispute case, a CFS was brought in by a large computer services corporation to perform a forensic recovery on an employee's desktop computer. The client suspected the employee, who was a foreign national, of hacking into other classified computer systems based on information generated by the client's external auditing software program. How did the CFS go about conducting the investigation?

HANDS-ON PROJECTS

After finding pornography downloaded on its network server and a number of individual office computers, a client began to build a case for employee dismissal. A CFS team (CFST) was hired to locate any deleted files and verify certain illicit and non-work-related contents of the hard drives in question. How did the CFST go about conducting their examination?

Case Project

After being sued for negligence, a client was about to settle a multimillion dollar suit and rewrite their entire software package because the plaintiff was charging that the installation of the software in question had permanently damaged/erased existing files; the irreplaceable data was not recoverable by any means and the plaintiff could not access files in a specific software application critical to running his business. How did the CFS go about conducting the investigation?

Optional Team Case Project

Five fire-damaged UNIX server drives were literally shoveled out of the debris from a large auto dealership. The backup tapes (plastic-material) had been co-located with the server drives and were themselves destroyed. All financial data (inventory, accounts payable and receivable, W-2s, customers and loan information) was destroyed. How was the CFS able to go about recovering the data?

REFERENCES

[1] Vacca, John R., *Firewalls: Jumpstart for Network and Systems Administrators,* Elsevier Digital Press, Burlington, MA, 2004.

[2] Vacca, John R., *i-mode Crash Course*, McGraw-Hill, New York, 2002.

[3] Vacca, John R., *Wireless Broadband Networks Handbook*, McGraw-Hill, New York, 2001.

[4] Vacca, John R., *Electronic Commerce,* 3rd ed., Charles River Media, Hingham, MA, 2001.

[5] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

[6] Vacca, John R., *Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan*, McGraw-Hill, New York, 2001.

17 The Information Warfare Arsenal of the Future

Terrorists take control of the New York Stock Exchange? Terrorism over the Internet? Computer viruses in the arsenal of Hizballah? As discussed in preceding chapters, such possibilities are currently being discussed by strategic analysts under the catch-all title of "information warfare." To date, the defense establishment has yet to agree on the exact definition of the term *information warfare*.

Only the entertainment industry, in the form of films and novels, has popularized the notion of an electronic doomsday scenario in which covert terrorist groups manage to penetrate critical nodes of the national information infrastructure (NII) and defense information infrastructure (DII) and are able to, variously, launch nuclear weapons, crash the telephone system, cause mayhem on the railways or in the air, or bring the financial sector to a catastrophic halt (see sidebar, "Will the Real La Femme Nikita Please Stand Up?"). Warnings also come from more sober sources. In 1999 the U.S. Joint Chiefs of Staff concluded that the convergence of vulnerable information infrastructures with traditional critical infrastructures had created a tunnel of vulnerability previously unrealized in the history of conflict. In other words, the one thing that everyone agrees on is that in the digital age, information, and its dissemination, has achieved the status of a vital strategic asset.

WILL THE REAL LA FEMME NIKITA PLEASE STAND UP?

Section One (in the USA Network's series *La Femme Nikita*) was the most covert antiterrorism organization on the planet. ABC's *Alias* and Fox's *24*, don't hold a candle to *La Femme Nikita* when it comes to wholesale assassinations and torture. Section

→

One is a skilled team of operatives responsible for protecting human life around the globe from chaos and destruction.

Sound implausible? Maybe. But the creation of such covert antiterrorism organizations are currently in the planning stages by the National Security Agency (NSA) and the CIA. NSA and the CIA realize that conventional information warfare (IW) tactics will not be enough in the future to thwart the very dangerous and often suicidal covert terrorist organizations. Like the character Nikita, who "transforms into a highly trained agent dedicated to fighting global terrorism by any means necessary—legal or otherwise," today's agents will have to do the same.

In the very near future, agents trained and armed with an arsenal of futuristic high-tech weapons and trained in the most sophisticated techniques for carrying out successful assassinations will swoop down upon deadly terrorist operatives. Like Nikita, they will all have to be the perfect weapon. They will also have to keep their wits about them, as well as ingenuity to keep themselves alive, where a single mistake could mean death. This will be their most vital weapon—and the best hope for the future of all that is good in the world.

If the response of the American defense establishment is any indication, strategic analysts are taking the possibilities of infowar seriously. The first global cyberwar will be like no other war ever fought before—where the enemy is invisible, the battles virtual, and the casualties all too real. Special committees in every branch of the U.S. armed forces are studying the potential of infowar, both as a defensive and an offensive weapon. The NSA is reportedly studying a rather imaginative arsenal of "info-weapons." Among the current possible offensive weapons are:

- Computer viruses, which could be fed into an enemy's computers either remotely or by "mercenary" technicians
- Logic bombs, another type of virus that can lie dormant for years, until, upon receiving a particular signal, it would wake up and begin attacking the host system
- "Chipping," a plan (originally proposed by the CIA, according to some sources) to slip booby-trapped computer chips into critical systems sold by foreign contractors to potentially hostile third parties (or recalcitrant allies?)
- Worms, whose purpose is to self-replicate ad infinitum, thus eating up a system's resources
- Trojan horses, malevolent code inserted into legitimate programming to perform a disguised function
- Back doors and trap doors, a mechanism built into a system by the designer to give the manufacturer or others the ability to sneak back into the system at a later date by circumventing the need for access privileges

A few other goodies in the arsenal of IW are devices for disrupting data flow or damaging entire systems, hardware and all. Among these, as explained in earlier chapters, are high energy radio frequency (HERF) guns, which focus a high power radio signal on target equipment, putting it out of action, and electromagnetic pulse (EMP) devices, which can be detonated in the vicinity of a target system. Such devices can destroy electronics and communications equipment over a wide area.

All of the preceding current and future offensive and defensive IW weapons arsenal will be discussed in specific detail next.

WEAPONS OF THE FUTURE

Body count: 796. Cause: midair collision. The air traffic control system was "cybotaged." News reports indicate that FAA personnel complained that their radar screens were freezing and were switching data tags (such as aircraft altitude data) between close-flying planes, causing a series of near-misses in skies throughout the country—and one head-on collision between passenger jets in a thunderstorm over New York, resulting in the deaths of all aboard. It's suspected that the automated route and altitude management program's collision-avoidance algorithm was damaged.

Body count: 1,807. Cause: midair collision with a structure. The navigation system of another passenger jet was taken over by hackers, leaving the pilots helpless as the jet nose-dived into the Sears Tower in Chicago. No reports yet on how the hackers got in. A couple of hit sites have posted theories, some of them pretty good.

A message posted to 90,000 newsgroups from a group known as "The Vulture of Jihad" claimed credit for the attack. As they're an obscure Sunni sect known for abjuring the use of any technology, their claim, made during prayers in a mosque in Aleppo, was disregarded. Other Islamic splinter groups also claimed credit, along with a white supremacist faction and an anarchist syndicate. These claims were swiftly dismissed, too: all were missing the digital signature that the Islamic Liberation Army (ILA) had in both previous site hacks. The most outrageous theory as to the identity of the people responsible for the attack came on a hit site called the Hit Theorist. It says the whole thing is a CIA, NSA, and Department of Defense (DoD) plot to generate support in Congress for increased spending of military and Black Ops operations.

Do these scenarios sound like spin-offs from Fox's *X-Files*' "The Lone Gunmen"? Perhaps. But could it happen? You bet.

The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction

Perhaps the most dangerous of all of defensive and offensive weapons in the IW arsenal of the future is the electromagnetic bomb. High-power EMP generation techniques and high-power microwave (HPM) technology have matured to the point where practical E-bombs (electromagnetic bombs) are becoming technically feasible, with new applications in both strategic and tactical information warfare. The development of conventional E-bomb devices allows their use in nonnuclear confrontations. This section discusses aspects of the technology base and weapon delivery techniques and proposes a foundation for the use of such devices in warhead and bomb applications.

The efficient execution of an IW campaign against a modern industrial or postindustrial opponent will require the use of specialized tools designed to destroy information systems. Electromagnetic bombs (also popularized by the USA network's sci-fi show *Dark Angel*) can provide, where delivered by suitable means, an effective tool for this purpose.

The EMP Effect

The EMP effect was first observed during the early testing of high-altitude airburst nuclear weapons. The effect is characterized by the production of a very short (hundreds of nanoseconds) but intense EMP, which propagates away from its source with ever-diminishing intensity, governed by the theory of electromagnetism. The EMP is, in effect, an electromagnetic shock wave.

NOTE

EMP stands for electromagnetic pulse. The source can be a nuclear or a nonnuclear detonation. It can be used by special forces teams who infiltrate the enemy's territory and detonate a device near their electronic devices. It destroys the electronics of all computer and communication systems in a quite large area. The EMP bomb can be smaller than a HERF gun to cause a similar amount of damage and is typically used to damage not a single target (not aiming in one direction) but to damage all equipment near the bomb.

This pulse of energy produces a powerful electromagnetic field, particularly within the vicinity of the weapon burst. The field can be sufficiently strong to produce short-lived transient voltages of thousands of volts (kiloVolts) on exposed electrical conductors, such as wires, or conductive tracks on printed circuit boards, where exposed.

It is this aspect of the EMP effect that is of military significance, as it can result in irreversible damage to a wide range of electrical and electronic equipment, particularly computers and radio or radar receivers. Subject to the electromagnetic hardness of the electronics, a measure of the equipment's resilience to this effect, and the intensity of the field produced by the weapon, the equipment can be irreversibly damaged or, in effect, electrically destroyed. The damage inflicted is not unlike that experienced through exposure to close proximity lightning strikes and may require complete replacement of the equipment, or at least substantial portions thereof.

Commercial computer equipment is particularly vulnerable to EMP effects, as it is largely built up of high-density metal oxide semiconductor (MOS) devices, which are very sensitive to exposure to high-voltage transients. What is significant about MOS devices is that very little energy is required to permanently wound or destroy them; any voltage typically in excess of ten volts can produce an effect termed "gate breakdown," which effectively destroys the device. Even if the pulse is not powerful enough to produce thermal damage, the power supply in the equipment will readily supply enough energy to complete the destructive process. Wounded devices may still function, but their reliability will be seriously impaired. Shielding electronics with equipment chassis provides only limited protection, as any cables running in and out of the equipment will behave very much like antennae, in effect, guiding the high-voltage transients into the equipment.

Computers used in data processing systems; communications systems; displays; industrial control applications, including road and rail signaling; and those embedded in military equipment, such as signal processors, electronic flight controls, and digital engine control systems, are all potentially vulnerable to the EMP effect.

Other electronic devices and electrical equipment may also be destroyed by the EMP effect. Telecommunications equipment can be highly vulnerable, because of the presence of lengthy copper cables between devices [1]. Receivers of all varieties are particularly sensitive to EMP, as the highly sensitive miniature high-frequency transistors and diodes in such equipment are easily destroyed by exposure to high-voltage electrical transients. Therefore, radar and electronic warfare equipment, satellite, microwave, UHF, VHF, HF, and low-band communications equipment and television equipment are all potentially vulnerable to the EMP effect. Modern military platforms are densely packed with electronic equipment, and unless these platforms are well hardened, an EMP device can substantially reduce their function or render them unusable.

The Technology Base for Conventional Electromagnetic Bombs

The technology base that may be applied to the design of electromagnetic bombs is both diverse and in many areas quite mature. Key technologies that are extant in the area are explosively pumped flux compression generators (FCGs), explosive or propellant driven magneto-hydrodynamic (MHD) generators, and a range of HPM devices, the foremost of which is the virtual cathode oscillator or vircator. A wide range of experimental designs have been tested in these technology areas, and a considerable volume of work has been published in unclassified literature.

This section will review the basic principles and attributes of these technologies in relation to bomb and warhead applications. This treatment is not exhaustive and is only intended to illustrate how the technology base can be adapted to an operationally deployable capability.

The Lethality of Electromagnetic Warheads

The issue of electromagnetic weapon lethality is complex. Unlike the technology base for weapon construction, which has been widely published in the open literature, lethality-related issues have been published much less frequently.

Although the calculation of electromagnetic field strengths achievable at a given radius for a given device design is a straightforward task, determining a kill probability for a given class of target under such conditions is not. This is for good reasons. The first is that target types are very diverse in their electromagnetic hardness, or ability to resist damage. Equipment that has been intentionally shielded and hardened against electromagnetic attack will withstand greater orders of magnitude and field strengths than standard commercially rated equipment. Moreover, various manufacturer's implementations of like types of equipment may vary significantly in hardness because of idiosyncrasies of specific electrical designs, cabling schemes, and chassis/shielding designs used.

The second major problem area in determining lethality is that of coupling efficiency, which is a measure of how much power is transferred from the field produced by the weapon into the target. Only power coupled into the target can cause useful damage.

Targeting Electromagnetic Bombs

The task of identifying targets for attack with electromagnetic bombs can be complex. Certain categories of target will be very easy to identify and engage. Buildings housing government offices and thus computer equipment, production facilities, military bases, and known radar sites and communications nodes are all targets that can be readily identified through conventional photographic, satellite, imaging radar, electronic reconnaissance, and human operations. These targets are typically geographically fixed and thus may be attacked, providing that the aircraft can penetrate to weapon release range. With the accuracy inherent in global positioning system (GPS)/inertially guided weapons, the electromagnetic bomb can be programmed to detonate at the optimal position to inflict a maximum of electrical damage.

Mobile and camouflaged targets that radiate overtly can also be readily engaged. Mobile and relocatable air defense equipment, mobile communications nodes [2], and naval vessels are all good examples of this category of target. While radiating, their positions can be precisely tracked with suitable electronic support measures (ESMs) and emitter locating systems (ELSs) carried either by the launch platform or a remote surveillance platform. In the latter instance, target coordinates can be continuously datalinked to the launch platform. As most such targets move relatively slowly, they are unlikely to escape the footprint of the electromagnetic bomb during the weapon's flight time.

Mobile or hidden targets that do not overtly radiate may present a problem, particularly should conventional means of targeting be employed. A technical solution to this problem does, however, exist for many types of target. This solution is the detection and tracking of unintentional emission (UE). UE has attracted the most attention in the context of TEMPEST surveillance, where transient emanations leaking out from equipment because of poor shielding can be detected and, in many instances, demodulated to recover useful intelligence. Termed "Van Eck radiation," such emissions can only be suppressed by rigorous shielding and emission-control techniques, such as are employed in TEMPEST rated equipment.

Although the demodulation of UE can be a technically difficult task to perform well, in the context of targeting electromagnetic bombs this problem does not arise. To target such an emitter for attack requires only the ability to identify the type of emission and thus target type and to isolate its position with sufficient accuracy to deliver the bomb. Because the emissions from computer monitors, peripherals, processor equipment, switchmode power supplies, electrical motors, internal combustion engine ignition systems, variable duty cycle electrical power controllers (thyristor or triac-based), superheterodyne receiver local oscillators, and computer networking cables are all distinct in their frequencies and modulations, a suitable ELS can be designed to detect, identify, and track such sources of emission.

A good precedent for this targeting paradigm exists. During the SEA (Vietnam) conflict, the U.S. Air Force operated a number of night interdiction gunships that used direction-finding receivers to track the emissions from vehicle ignition systems. Once a truck was identified and tracked, the gunship would engage it.

Because UE occurs at relatively low power levels, the use of this detection method prior to the outbreak of hostilities can be difficult, as it may be necessary to overfly hostile territory to find signals of usable intensity. The use of stealthy reconnaissance aircraft or long-range, stealthy unmanned aerial vehicles (UAVs) may be required. The latter also raises the possibility of autonomous electromagnetic-warhead-armed expendable UAVs, fitted with appropriate homing receivers. These would be programmed to loiter in a target area until a suitable emitter is detected, upon which the UAV would home in and expend itself against the target.

The Delivery of Conventional Electromagnetic Bombs

As with explosive warheads, electromagnetic warheads will occupy a volume of physical space and will also have some given mass (weight) determined by the density of the internal hardware. Like explosive warheads, electromagnetic warheads may be fitted to a range of delivery vehicles.

Known existing applications involve fitting an electromagnetic warhead to a cruise missile airframe. The choice of a cruise missile airframe will restrict the weight of the weapon to about 340 kg (750 lb), although some sacrifice in airframe fuel capacity could see this size increased. A limitation in all such applications is the need to carry an electrical energy storage device (a battery), to provide the current used to charge the capacitors used to prime the FCG prior to its discharge. Therefore, the available payload capacity will be split between the electrical storage and the weapon itself.

In wholly autonomous weapons such as cruise missiles, the size of the priming current source and its battery may well impose important limitations on weapon capability. Air-delivered bombs, which have a flight time between tens of seconds to minutes, could be built to exploit the launch aircraft's power systems. In such a bomb design, the bomb's capacitor bank can be charged by the launch aircraft en route to the target, and after release a much smaller onboard power supply could be used to maintain the charge in the priming source prior to weapon initiation.

An electromagnetic bomb delivered by a conventional aircraft can offer a much better ratio of electromagnetic device mass to total bomb mass, as most of the bomb mass can be dedicated to the electromagnetic-device installation itself. It follows, therefore, that for a given technology an electromagnetic bomb of identical mass to an electromagnetic-warhead-equipped missile can have a much greater lethality, assuming equal accuracy of delivery and technologically similar electromagnetic device design.

A missile-borne electromagnetic warhead installation will be composed of the electromagnetic device, an electrical energy converter, and an onboard storage device such as a battery. As the weapon is pumped, the battery is drained. The electromagnetic device will be detonated by the missile's onboard fusing system. In a cruise missile, this will be tied to the navigation system; in an antishipping missile, the radar seeker; and in an air-to-air missile, the proximity fusing system. The warhead fraction (ratio of total payload [warhead] mass to launch mass of the weapon) will be between 15% and 30%.

An electromagnetic bomb warhead will be composed of an electromagnetic device, an electrical energy converter, and an energy storage device to pump and sustain the electromagnetic device charge after separation from the delivery platform. Fusing could be provided by a radar altimeter fuse to airburst the bomb, a barometric fuse, or in GPS/inertially guided bombs, the navigation system. The warhead fraction could be as high as 85%, with most of the usable mass occupied by the electromagnetic device and its supporting hardware.

Because of the potentially large lethal radius of an electromagnetic device compared to an explosive device of similar mass, standoff delivery would be prudent. Although this is an inherent characteristic of weapons such as cruise missiles, potential applications of these devices to glidebombs, antishipping missiles, and air-to-air missiles would dictate fire and forget guidance of the appropriate variety to allow the launching aircraft to gain adequate separation of several miles before warhead detonation.

The recent advent of GPS satellite [3] navigation guidance kits for conventional bombs and glidebombs has provided the optimal means for cheaply delivering such weapons. Although GPS-guided weapons without differential GPS enhancements may lack the pinpoint accuracy of laser- or television-guided munitions, they are still quite accurate (circular error probable [CEP]\(~40 ft), cheap, and autonomous all-weather weapons.

The U.S. Air Force has deployed the Northrop GPS-aided munition (GAM) on the B-2 bomber as well as the GPS/inertially guided GBU-29/30 joint direct attack munition (JDAM) and the AGM-154 joint stand-off weapon (JSOW) glidebomb. Other countries are also developing this technology. For example, the Australian BAeA agile glide weapon (AGW) glidebomb is achieving a glide range of about 140 km (75 nautical miles [nmi]) when launched from that altitude.

The importance of glidebombs as delivery means for HPM warheads is threefold. First, the glidebomb can be released from outside the effective radius of target air defenses, therefore minimizing the risk to the launch aircraft. Second, the large standoff range means that the aircraft can remain well clear of the bomb's effects. Finally the bomb's autopilot may be programmed to shape the terminal trajectory of the weapon, such that a target may be engaged from the most suitable altitude and aspect.

A major advantage of using electromagnetic bombs is that they may be delivered by any tactical aircraft with a nav-attack system capable of delivering GPS-guided munitions. As you can expect GPS-guided munitions to become the standard weapon in use by Western air forces in the 21st century, every aircraft capable of delivering a standard guided munition also becomes a potential delivery vehicle for an electromagnetic bomb. Should weapon ballistic properties be identical to the standard weapon, no software changes to the aircraft would be required.

Because of the simplicity of electromagnetic bombs in comparison with weapons such as anti-radiation missiles (ARMs), it is not unreasonable to expect that these should be both cheaper to manufacture and easier to support in the field, thus allowing for more substantial weapon stocks. In turn, this makes saturation attacks a much more viable proposition.

Defense Against Electromagnetic Bombs

The most effective defense against electromagnetic bombs is to prevent their delivery by destroying the launch platform or delivery vehicle, as is the case with nuclear weapons. This, however, may not always be possible, and therefore systems that can be expected to suffer from exposure to the electromagnetic weapons' effects must be electromagnetically hardened.

The most effective method is to wholly contain the equipment in an electrically conductive enclosure, termed a "Faraday cage," which prevents the electromagnetic field from gaining access to the protected equipment. However, most such equipment must communicate with and be fed with power from the outside world, and this can provide entry points via which electrical transients may enter the enclosure and cause damage. Although optical fibers address this requirement for transferring data in and out, electrical power feeds remain an ongoing vulnerability.

Where an electrically conductive channel must enter the enclosure, electromagnetic-arresting devices must be fitted. A range of devices exist, but care must be taken in determining their parameters to ensure that they can deal with the rise time and strength of electrical transients produced by electromagnetic devices. Reports from the United States indicate that hardening measures attuned to the behavior of nuclear EMP bombs do not perform well when dealing with some conventional microwave electromagnetic device designs.

Hardening of systems must be carried out at a system level, as electromagnetic damage to any single element of a complex system could inhibit the function of the whole system. Hardening new building equipment and systems will add a substantial cost burden. Older equipment and systems may be impossible to harden properly or may require complete replacement. In simple terms, hardening by design is significantly easier than attempting to harden existing equipment.

An interesting aspect of electrical damage to targets is the possibility of wounding semiconductor devices, thereby causing equipment to suffer repetitive intermittent faults rather than complete failures. Such faults would tie down considerable maintenance resources while also diminishing the confidence of the operators in the equipment's reliability. Intermittent faults may not be economically possible to repair, thereby causing equipment in this state to be removed from service permanently, with considerable loss in maintenance hours during damage diagnosis. This factor must also be considered when assessing the hardness of equipment against electromagnetic attack, as partial or incomplete hardening may, in this fashion, cause more difficulties than it would solve. Indeed, shielding that is incomplete may resonate when excited by radiation and thus contribute to damage inflicted on the equipment contained within it.

Other than hardening against attack, facilities that are concealed should not radiate readily detectable emissions. Where radio frequency communications must be used, low probability of intercept (spread spectrum) techniques should be employed exclusively to preclude the use of site emissions for electromagnetic-targeting purposes. Appropriate suppression of UE is also mandatory.

Communications networks for voice, data, and services should employ topologies with sufficient redundancy and failover mechanisms to allow operation with multiple nodes and links inoperative. This will deny a user of electromagnetic bombs the option of disabling large portions if not the whole of the network by taking down one or more key nodes or links with a single or small number of attacks.

Limitations of Electromagnetic Bombs

The limitations of electromagnetic weapons are determined by weapon implementation and means of delivery. Weapon implementation will determine the electromagnetic field strength achievable at a given radius and its spectral distribution. Means of delivery will constrain the accuracy with which the weapon can be positioned in relation to the intended target. Both constrain lethality.

In the context of targeting military equipment, it must be noted that thermionic technology (vacuum tube equipment) is substantially more resilient to the electromagnetic weapons effects than solid-state (transistor) technology. Therefore, a weapon optimized to destroy solid-state computers and receivers may cause little or no damage to a thermionic technology device, for instance early-1960s Soviet military equipment. Therefore, a hard electrical kill may not be achieved against such targets unless a suitable weapon is used.

This underscores another limitation of electromagnetic weapons, which is the difficulty in kill assessment. Radiating targets such as radars or communications equipment may continue to radiate after an attack even though their receivers and data processing systems have been damaged or destroyed. This means equipment that has been successfully attacked may still appear to operate. Conversely, an opponent may shut down an emitter if attack is imminent, and the absence of emissions means that the success or failure of the attack may not be immediately apparent.

Assessing whether an attack on a nonradiating emitter has been successful is more problematic. A good case can be made for developing tools specifically for the purpose of analyzing unintended emissions, not only for targeting purposes but also for kill assessment.

An important factor in assessing the lethal coverage of an electromagnetic weapon is atmospheric propagation. Although the relationship between electromagnetic field strength and distance from the weapon is one of an inverse square law in free space, the decay in lethal effect with increasing distance within the atmosphere will be greater because of quantum physical absorption effects. This is particularly so at higher frequencies, and significant absorption peaks caused by water vapor and oxygen exist at frequencies above 20 GHz. These will therefore contain the effect of HPM weapons to shorter radii than are ideally achievable in the K and L frequency bands.

Means of delivery will limit the lethality of an electromagnetic bomb by introducing limits to the weapon's size and the accuracy of its delivery. Should the delivery error be of the order of the weapon's lethal radius for a given detonation altitude, lethality will be significantly diminished. This is of particular importance when assessing the lethality of unguided electromagnetic bombs, as delivery errors will be more substantial than those experienced with guided weapons such as GPS-guided bombs.

Therefore, accuracy of delivery and achievable lethal radius must be considered against the allowable collateral damage for the chosen target. Where collateral electrical damage is a consideration, accuracy of delivery and lethal radius are key parameters. An inaccurately delivered weapon of large lethal radius may be unusable against a target should the likely collateral electrical damage be beyond acceptable limits. This can be a major issue for users constrained by treaty provisions on collateral damage.

The Proliferation of Electromagnetic Bombs

At the time of this writing, the United States is one of several nations with the established technology base and the depth of specific experience to design weapons based upon this technology. However, the relative simplicity of the FCG and the vircator suggests that any nation with even a 1940s technology base, once in possession of engineering drawings and specifications for such weapons, could manufacture them.

As an example, the fabrication of an effective FCG can be accomplished with basic electrical materials, common plastic explosives such as C-4 or Semtex, and readily available machine tools such as lathes and suitable mandrels for forming coils. Disregarding the overheads of design, which do not apply in this context, a two-stage FCG could be fabricated for a cost as low as $14,000–15,000 at Western labor rates. This cost could be even lower in a third world or newly industrialized economy.

Although the relative simplicity and thus low cost of such weapons can be considered of benefit to first world nations intending to build viable war stocks or maintain production in wartime, the possibility of less developed nations mass producing such weapons is alarming. The dependence of modern economies upon first world nations' information technology infrastructures, makes them highly vulnerable to attack with such weapons, providing that such weapons can be delivered to their targets.

Of major concern is the vulnerability resulting from the increasing use of communications and data communications schemes based on copper cable media. If the copper media were to be replaced en masse with optical fiber to achieve higher bandwidths, the communications infrastructure would become significantly more robust against electromagnetic attack. However, the current trend is to exploit existing distribution media such as cable TV and telephone wiring to provide multiple megabit/s data distribution (cable modems, ADSL/HDSL/VDSL) to premises. Moreover, the gradual replacement of coaxial

Ethernet networking with 10-Base-T twisted pair equipment has further increased the vulnerability of wiring systems inside buildings. It is not unreasonable to assume that the data and services communications infrastructure in the West will remain a "soft" electromagnetic target in the foreseeable future.

At this time, no counter-proliferation regimes exist. Should treaties be agreed upon to limit the proliferation of electromagnetic weapons, they would be virtually impossible to enforce, given the common availability of suitable materials and tools.

With the former Soviet Union suffering significant economic difficulties, the possibility of microwave and pulse power technology designs leaking out to third world nations or terrorist organizations should not be discounted. The threat of electromagnetic bomb proliferation is very real.

A Doctrine for the Use of Conventional Electromagnetic Bombs

A fundamental tenet of IW is that complex organizational systems such as governments, industries, and military forces cannot function without the flow of information through their structures. Information flows within these structures in several directions under typical conditions of function. A trivial model for this function would see commands and directives flowing outward from a central decision-making element, with information about the state of the system flowing in the opposite direction. Real systems are substantially more complex.

This is of military significance because stopping this flow of information will severely debilitate the function of any such system. Stopping the outward flow of information produces paralysis, as commands cannot reach the elements that are to execute them. Stopping the inward flow of information isolates the decision-making element from reality and thus severely inhibits its capacity to make rational decisions that are sensitive to the currency of information at hand.

The recent evolution of strategic (air) warfare indicates a growing trend toward targeting strategies that exploit this most fundamental vulnerability of any large and organized system. The Desert Storm air war of 1991 is a good example, with a substantial effort expended against such targets. Indeed, the model used for modern strategic air attack places leadership and its supporting communications in the position of highest targeting priority. No less important, modern electronic combat concentrates on the disruption and destruction of communications and information-gathering sensors used to support military operations. Again, the Desert Storm air war provides a good illustration of the application of this method.

A strategy that stresses attack on the information-processing and communications elements of the targeted systems offers a very high payoff, as it will introduce an increasing level of paralysis and disorientation within its target. Electromagnetic bombs are a powerful tool in the implementation of such a strategy.

Computer Viruses

A virus is a code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces.

Viruses are well known in every computer-based environment, so it is not astonishing that this type of rough program is used in IW. One could imagine that the CIA (or Army, Air Force, etc.) inserts computer viruses into the switching networks of the enemy's phone system. As today's telephone systems are switched by computers, you can shut them down, or at least cause massive failure, with a virus as easily as you can shut down a computer.

Worms

A worm is an independent program. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually doesn't modify other programs.

If worms don't destroy data, they can cause the loss of communication by merely eating up resources and spreading through networks. A worm can also easily be modified so that data deletion or worse occurs. With a "wildlife" like this, you could imagine breaking down a networked environment such as an ATM and banking network.

Trojan Horses

A trojan horse is a code fragment that hides inside a program and performs a disguised function. It's a popular mechanism for disguising a virus or a worm.

A trojan horse could be camouflaged as a security-related tool. If someone edits this program so that it sends discovered security holes in an email message back to him (password file could also be included), the cracker acquired much information about vulnerable hosts and servers. A cleverly written trojan horse does not leave traces of its presence and, because it does not cause detectable damage, it is hard to detect.

Logic Bombs

A logic bomb is a type of trojan horse used to release a virus, a worm, or some other system attack. It's either an independent program or a piece of code that's been planted by a system developer or programmer.

With the overwhelming existence of U.S.-based software (MS Windows or UNIX systems), the U.S. government, or whomever you would like to imagine, could decide that no software would be allowed to be exported from that country without a trojan horse. This hidden function could become active when a document with "war against the USA" exists on the computer. Its activation could also be triggered from the outside. An effect could be to format the computers hard disks or to mail the document to the CIA.

Trap Doors

A trap door, or a back door, is a mechanism that's built into a system by its designer. The function of a trap door is to give the designer a way to sneak back into the system, circumventing normal system protection.

As previously mentioned, all U.S. software could be equipped with a trap door that would allow IW agencies to explore systems and the stored data on foreign countries. This could be most useful in cases of military strategic simulations and plans and would provide the DoD's intelligence with vital information.

Chipping

Just as software can contain unexpected functions, it is also possible to implement similar functions in hardware. Today's chips contain millions of integrated circuits that can easily be configured by the manufacturer so that they also contain some unexpected functions. They could be built so that they fail after a certain time, blow up after they receive a signal on a specific frequency, or send radio signals that allow identification of their exact location— the number of possible scenarios exceeds, by far, the scope of this chapter. The main problem with chipping is that the specific (adapted) chip be installed in the place that is useful for the information warrior in making detection possible. The easiest solution is to build the additional features into all the chips manufactured in the country that is interested in this type of IW.

Nano Machines and Microbes

In the future, nano machines [4] and microbes will provide the possibility to cause serious harm to a system. Unlike viruses, you can use these to attack not the software but the hardware of a computer system. Nano machines are tiny robots (smaller than ants) that could be spread at an information center of the enemy. They crawl through the halls and offices until they find a computer. They are so small that they enter the computer through slots and shut down electronic circuits.

Another way to damage the hardware is a special breed of microbes. This special breed of microbes can eat oil, but what if they were bred for eating silizium? They would destroy all integrated circuits in a computer lab, a site, a building, a town, and so on. Nano technology and microbes will be discussed in much greater detail later in the chapter.

Electronic Jamming

In the old days (and even today) electronic jamming was used to block communications channels at the enemy's equipment so that they couldn't receive any information. The next step is not to block their traffic, but, instead, overwhelm them with incorrect information—otherwise known as disinformation.

THE GLOBAL POSITIONING SYSTEM

GPS receivers, one of the newest and probably most important of the IW toys for Big Brother and the boys, will be everywhere soon—in cars, boats, planes, backpacks, briefcases, purses, jackets, and pants pockets. The good news is, you'll always know exactly where you are. The bad news is, so will everyone else.

Most humans who have ever lived have known roughly where they were, day-by-day, year-by-year. Not in abstract terms, of course, but in the terms of experience and familiarity—by neighborhood, not map. For eons, we've known things about ourselves that could be expressed in a statement like "I'm standing on the threshing floor in the village of my birth" or "I'm walking across the mid-morning shadow cast by Notre Dame" or even "I'm in a part of town I've never seen before." Whether one utters it or not, this awareness of "whereness" is part of the meaning of being human, but for centuries, a dedicated band of mapmakers, navigators, astronomers, inventors, and mathematicians has tried to turn this innate sense of place into a more precise determination of position that is intelligible to anyone, not only to locals. On one level, this is like the difference between knowing you're coming to the corner where you always turn left on your way to the grocery store and knowing the names of the streets that cross at that intersection. On another level, however, the pursuit of pure position is about to lead us into a world that none of us has ever seen. The agent of change will be GPS—the global positioning system—which, like so many tools of the modern world, is both familiar and misunderstood at the same time.

Until recently, not a single human-made object has ever known where it was. Even a venerable tool of navigation such as a sextant knows nothing more about its location than does the *Mona Lisa* or the pigments from which she is painted. Imagine a world in which man-made objects know where they are and can communicate that information to other self-locating, communicating objects. This sounds as strange and surprising as the Marauder's Map in the Harry Potter novels [5]. The Marauder's Map shows the position and movement of every animate creature at the school of wizardry called Hogwarts. A Marauder's Map of the world would be even stranger. It would show the position and movement (even a history of movements) of man-made objects as well. This would be an ever-changing map or a world filled with artifacts busily announcing something significant about themselves to each other and to anyone else who cared to listen.

That world is here. In August 2000, a company called SiRF Technology based in Santa Clara, California, announced that it had developed an advanced GPS chip no bigger than a postage stamp. SiRF's vision is to bring location awareness to virtually everything that moves. This is a subtle but profound change in the history of GPS technology—a change driven, like everything else these days, by increasing miniaturization and declining prices for sophisticated circuitry. In the past few years, consumers have grown used to the sight of hand-held GPS receivers, which have been marketed as individual positioning devices for anglers, hunters, hikers, and cyclists. What SiRF and other companies have in mind, is conferring upon objects a communicable sense of place. One day soon, most GPS devices will not be stand-alone receivers used by those of us who venture off the beaten path, but integral components of everyday objects.

Some of these objects, especially the big ones, are easy enough to imagine, because they exist now. Boats and ships of every kind already incorporate GPS technology, as do some automobiles made by Toyota, Honda, Lexus, and Cadillac. So do the newest farm implements, such as combines that allow farmers to map crop yields in precise detail. Some uses of GPS that are not yet widely available will soon be common in smaller devices. For instance, the Federal Communications Commission requires cellular-phone service providers to be able to identify the location of a cell-phone caller who dials 911. This means that most cell phones now include a tiny GPS chip. So do beepers and watches and handheld digital assistants and other digital devices like Game Boy Colors, Tamagotchis (virtual game animals), dog collars, and, probably, handguns as well.

The spread of a technology such as GPS is easy enough to predict, but it's much harder to foresee what the effect of that spread may be. There's always a limit to how far one can see into the future of the tools being used, especially into a future where those tools become interlinked. There was a time (only as long ago as Bill Gates' first book) when the value of computers was believed to lie mainly in their stand-alone power, not in the networks they might form when linked together. Now there's the Internet and the World Wide Web, whose far-reaching implications are only dimly visible, but which have already transformed the way countries all over the world do business.

The development of GPS technologies may follow a similar pattern. It's already obvious how useful GPS is in discrete applications: for surveying and mapmaking, the tracking of commercial vehicles, maritime and aeronautic navigation, and for use by emergency rescue crews and archaeologists. There is simply no telling what it will mean when, on a planet full of location-aware objects, a way is found to coordinate all the data they send out. Awareness may be a metaphor when applied to inanimate objects, but the potential of that metaphor is entirely literal. In the meantime, for most of us, there is still a more basic question to be answered: Where did GPS technology come from and how does it work?

GPS depends on an array of 50 satellites (47 in regular use, plus spares) flying some 11,000 miles above Earth. They were put there by the DoD, which began the NAVSTAR global positioning system program in 1973. A version of GPS was first tested in 1964, when the Navy deployed a five-satellite prototype, called Transit, for submarines. It could take an hour and a half for a Transit satellite to saunter above the horizon and then another 10 or 15 minutes to fix the submarine's position. The current generation of satellites was built by the Boeing Company and Lockheed Martin, and each one orbits the planet in about 12 hours, cutting across the equatorial plane at an angle of roughly 55 degrees. The U.S. Air Force tracks the satellites from Colorado Springs, Colorado, Hawaii, and three other islands: Ascension in the South Atlantic, Diego Garcia in the Indian Ocean, and Kwajalein in the South Pacific. These ground stations provide the satellites with navigational information, which the next generation of satellites will be able to supply to each other. Ordinary users can track this constellation of satellites with one of several Web sites or with an appealing public-domain software program called Home Planet, which can map any satellite you choose, GPS or not, against a projection of the Earth's surface. You can also track the satellites with a GPS receiver.

In the world of GPS, knowing where you are, give or take a few meters, depends on knowing precisely when you are. Just as longitude couldn't be effectively calculated until 1764, when John Harrison's chronometer was tested on a voyage to Barbados, so GPS couldn't be created until there was a way to mount highly accurate clocks in stable orbits. The problem with finding longitude in Harrison's era was making a chronometer that could keep accurate time at one location (Greenwich, England) even while the ship carrying that chronometer was halfway around the globe. The chronometer provides a constant frame of reference for the celestial events that shift as a ship moves eastward or westward.

GPS satellites effortlessly provide a constant frame of reference. Each carries three or four ultra-precise clocks synchronized to GPS time—which is, essentially, coordinated universal time (UTC) without the leap seconds. The satellite clocks are accurate to within one-millionth of a second of UTC as kept by the U.S. Naval Observatory. The GPS receiver translates the time that the satellites transmit into local time. As far as most civilian users are concerned, GPS is more accurate for time than it is for position, and, in most cases, GPS is far more accurate for position than it is for altitude. In 1764, Greenwich time was available only in Greenwich (on the meridian running through England) and in the presence of a properly maintained chronometer, of which there were two. Now, GPS time is available globally to anyone with a receiver.

When you turn on a GPS receiver, it tunes itself to a radio signal called L1, which comes from any GPS satellite—usually one of four to eight—coasting above the horizon. The U.S. military and other authorized users also receive two encrypted signals—one from L1, another from a frequency called L2. Those extra signals are one of the reasons military users can fix their location more precisely than civilian users can. By measuring the time it takes a signal to reach it, a GPS receiver calculates what is called the pseudo-range to the transmitting satellite. With at least four satellites in view, and hence four pseudo-ranges (the minimum for determining accurate location plus time), a GPS receiver can compute its position using basic trigonometry. It can also calculate velocity by comparing location readings taken at different points in time.

The real value of GPS begins to emerge when you consider a GPS receiver's ability to compare where it is now with where it was moments or hours or days ago. When you begin to move, a GPS springs to life. It announces your directional bearing, average speed, approximate altitude, the estimated time to get to a named destination, the degree to which you're adhering to a planned path, and the distance to your destination—in short, it calibrates the dimensions of your dynamism or the dynamism of anything you attach it to, from a delivery truck to an outcropping of the Earth's crust. A navigator's task has always been to plot his current position, compare it with his previous day's position, and deduce from those two points some idea of tomorrow's position. These are the functions inherent, and almost instantly accessible, in a dynamic tracking system such as GPS. It's no wonder GPS has rapidly made its way into the navigation stations of recreational boats and commercial ships alike, replacing older electronic navigation systems as well as celestial navigation.

For civilian GPS users, there is a catch. The system is purposely compromised, its accuracy intentionally degraded. GPS was designed, as the responsible federal agencies are careful to remind us, to serve as a dual-use system with the primary purpose of enhancing the effectiveness of U.S. and allied military forces. One way to do that is to de-enhance everyone else's effectiveness—to deny nonmilitary users and foreign adversaries the kind of accuracy that military users enjoy, which in all kinds of targeting weapons is a difference of dozens of feet. This has been done by selectively and intermittently introducing error into the information GPS satellites dispense to receivers lacking access to the military's encrypted signals—in other words, to the receivers nonmilitary users and foreign adversaries can buy. One of the many ironies of GPS, however, is that a system designed mainly for military use and developed through the DoD at a cost of more than $10 billion has been engulfed by the commercial market. The result is that "selective availability," as GPS's intentional error is called, will most likely be phased out within the next decade.

The more positional signals a GPS receives, the more accurate it is. That's one reason why in 1999, then Vice President Gore, announced a $600 million initiative that would help fund additional civilian signals on GPS satellites scheduled for launch in the next decade—a clear acknowledgment of the scientific, commercial, and economic importance of nonmilitary GPS. Even at present, there are ways around selective availability. Some GPS receivers have been manufactured that can also tune in to the Russian equivalent of GPS, called GLONASS, which operates without signal compromise but lacks the reliability of GPS. The most common solution is differential GPS, or DGPS, in which "differential corrections" (indications of the degree of error at one station) are transmitted to GPS receivers via a radio link, greatly enhancing their accuracy regardless of selective availability. Even DGPS chips have shrunk to the size of postage stamps.

The U.S. Coast Guard operates a maritime DGPS service available to civilians, and the Federal Aeronautics Administration is implementing a similar system, called the Wide Area Augmentation System, which uses satellites as well as ground stations. Once a complementary system called Local Area Augmentation Service is in place at selected airports, the FAA will eventually be able to turn over the task of flight navigation, from takeoff to precision landings, entirely to GPS. The result of this is a bizarre irony, in which some branches of the federal government are working hard to offset error purposely created by another federal agency, the DoD.

GPS, especially DGPS, has come as a particular godsend to geophysicists, the men and women who study the physical and dynamic parameters of planet Earth. Most of us think of the Earth as an inherently stable platform: bedrock. To geophysicists, Earth experiences a wide range of volatility—some of it very slow, some of it occurring at the rate of days or weeks. Tectonic plates grind at each other's edges, cresting upward. Portions of the crust are still rebounding from the weight of long-vanished ice sheets. It adjusts locally to the shock of earthquakes and volcanoes. As a geophysicist might write: The torques from the sun, moon, and planets move the rotation axis of Earth in space. Torques from the atmosphere, ocean, and fluid core move the rotation axis relative to the crust of Earth. Both sources of torques change the rotation rate of Earth. GPS offers an extraordinary leap in the rate of data collection, with a corresponding leap in the understanding of Earth's motion.

As technology becomes more sophisticated, it seems as though freedom gets defined in more basic terms. GPS offers one version of freedom—knowing where you are—but it may ultimately threaten a more basic kind of freedom—being where you are without anyone else knowing it. Everyone would like to have a Marauder's Map, but no one wants to appear on the Marauder's Map without approving it. The value of cell- phones embedded with GPS chips is obvious when it comes to emergency services, but the cell-phone service providers' ability to track the location of a 911 call means that GPS could track the location of every other kind of call as well. Already, GPS is being used to monitor the movement of commercial trucks of every description. This is both a form of insight to the vehicle owners and a form of intrusion to the drivers, who find their movements visible to management in a way they never were before. GPS is also being used in experimental programs to monitor the movements of parolees. There is only a difference of emphasis between tracking a parolee with a GPS and tracking a sales representative with the same tool. All of us have learned all too well in the past few decades that even innocuous information can be assembled in ways that make it dangerous. Location, movement, and time are not innocuous forms of information.

As technology advances, it abstracts us farther and farther from the earth we live on. All of us inhabit a world of the senses, a world infinitely full of sensory clues to our location and bearing. Directionality is implicit in our being. The very factors that influence Earth's rotation (the sun, moon, planets, atmosphere, oceans) influence our sense of orientation, if only we can remember how to know them. It is far easier, after all, to navigate by pushing a single button and reading the numbers on yet another of the small gray screens that crowd our lives. GPS may mean many wonderful things, but it may also mean yet another death for the powers of human observation.

Also, GPS may be an example of technology that reaches the market the moment it becomes unnecessary—at least where ordinary consumers are concerned. Now that the nonaqueous and nonarctic globe is mostly paved, and the population of people is as thick on the Earth as mold on month-old bread, a device has been invented at last that tells you where you are without having to ask strangers.

SNOOP, SNIFF, AND SNUFF TOOLS

There's a fine line in the difference between "snoop" and "sniff" tools. The meaning of "snuff" tools is obvious. Let's look at Sniffit first.

Snoop and Sniff Tools

Sniffit is a kind of a network packet sniffer and snooper. Packet sniffers are rather intriguingly named pieces of software that monitor network traffic. Under many networking protocols, data that you transmit gets split into small segments, or packets, and the Internet protocol (IP) address of the destination computer is written into the header of each packet. These packets then get passed around by routers and eventually make their way to the network segment that contains the destination computer.

As each packet travels around that destination segment, the network card on each computer on the segment examines the address in the header. If the destination address on the packet is the same as the IP address of the computer, the network card grabs the packet and passes it on to its host computer.

Promiscuous Network Cards

Packet sniffers work slightly differently. Instead of just picking up the packets that are addressed to them, they set their network cards to what's known as "promiscuous mode" and grab a copy of every packet that goes past. This lets the packet sniffers see all data traffic on the network segment to which they're attached—if they're fast enough to be able to process all that mass of data, that is. This network traffic often contains very interesting information for an attacker, such as user identification numbers and passwords, confidential data—anything that isn't encrypted in some way.

This data is also useful for other purposes. Network engineers use packet sniffers to diagnose network faults, for example, and those in security use packet sniffers for their intrusion detection software. That last application is a real case of turning the tables on the attackers: hackers use packet sniffers to check for confidential data; companies use packet sniffers to check for hacker activity. That has a certain elegant simplicity to it.

The thing that worries most people about Sniffit is how easy it is to install. It takes about three commands and three minutes to get this thing installed and running on a Linux machine. It even has a graphical user interface (not exactly pretty, but it is free). Like Nmap, Sniffit is easy to use and does exactly what it says it does: It sniffs your network and shows you what sort of data is getting passed around.

It is recommended that you install a packet sniffer and have a look at what sort of data you can see on your local network. Better still, get one of your network engineers to install it for you. They probably know of better, more professional sniffers and will be able to talk you through some of the data that you see going past. It's an interesting look into exactly what's going on within your network.

Sniff

Security experts are still not convinced that Carnivore (the software created by the FBI to tap into Internet communications) is either ready to be used safely (without abuse) or can gather information that would be legally admissible in court. Although Carnivore is the best software available for the job today, it is perhaps not as good as it could be. Carnivore's source code should be made available for open review.

Such a review would provide confidence in Carnivore's ability to gather information accurately and fairly—confidence needed to make it a publicly accepted crime-fighting instrument. Unless it is demonstrated that Carnivore will enable surveillance personnel to obtain the information they are authorized to see, and not draw innocent bystanders into its net, it will remain an object of public suspicion.

The FBI publicly admitted the existence of Carnivore in July 2000, after it had been in use for over a year at numerous Internet service providers (ISPs) and rumors of its existence began to surface. Congress and privacy advocates then called for full disclosure of the software. Replying that such disclosure would only help criminals get around the system, the FBI offered to let it be reviewed by an outside technical group selected by the bureau. Illinois Institute of Technology's Research Institute (IITRI) was chosen after accepting the review limits proposed by the FBI, a stipulation other institutions such as the San Diego (California) Supercomputing Center would not accept.

The IITRI report does not address significant technical issues. Although it looks at how Carnivore worked when it was used as intended, the report failed to look at the larger issue: its system requirements. They did not look at the interaction between Carnivore and its host operating system or the interaction between Carnivore and the ISP's setup. Thus, the vulnerability of the system to hackers is still not clearly established.

Carnivore runs on Windows and to control it, the person who is using it must be logged on at the highest level: administrator. At that level, the operator (meant to be an FBI agent) has a great deal of freedom. For instance, he or she can access the content of all communications and change and edit files at will. What is more, anyone logged in as administrator can hide any evidence of the activity. Thus, it would be possible for an agent or someone who hacked into the system to tamper with evidence, plant false leads, or extract confidential information for bribery, extortion, fraud, and so on.

Failure to examine the interaction between Carnivore and an ISP's systems may be a gap in the report. The limited nature of IITRI's review cannot support a conclusion that Carnivore is accurate, safe, or always consistent with legal requirements. The scope of IITRI's review was dictated by the FBI, and any additional effort would have invalidated the contract under which the work was performed.

EMAIL WIRETAPS LIKE CARNIVORE CAN STEAL SENSITIVE CORRESPONDENCE

As part of its ongoing research, the Privacy Foundation (see sidebar, "The Privacy Foundation") found that a simple, hidden JavaScript code segment in HTML-formatted email messages can effectively allow someone to monitor all succeeding messages that are forwarded with the original message included. Clearly, this can cause confidential internal communications to be compromised. Here's a look at how to identify wiretaps and protect yourself from them.

THE PRIVACY FOUNDATION

The Privacy Foundation at the University of Denver conducts research into communications technologies and provides the public with tools to maintain privacy in the Information Age. You can read the Foundation's report and commentary on email wiretaps. The report cites the following possible uses for this security breach:

- The wiretaps can provide the ability to monitor the path of a confidential email message and the written comments attached.

→

- In a business negotiation conducted via email, one side can learn inside information from the other side as the proposal is discussed through the recipient company's internal email system.
- A bugged email message can capture thousands of email addresses as the forwarded message is sent around the world.
- Commercial entities, particularly those based offshore, may seek to offer email wiretapping as a service.

This security problem is a particularly dangerous one for organizations that conduct conversations containing sensitive internal information via email. The usual scenario for such communication is that a message from an outside source is forwarded from executive to executive within a company and it includes each person's comments. If there's an email wiretap on the original external document, each time someone forwards the message to someone else, a copy of their message is automatically and invisibly emailed to the original sender of the external message (or someone designated by him).

This problem affects only HTML-enabled email readers that have JavaScript turned on by default, such as Microsoft Outlook, Outlook Express, and Netscape Communicator. Eudora and AOL are not affected, nor are Web mail services such as Yahoo and Hotmail.

Snuff

As hackers obtain ever more dangerous and easy-to-use tools, they are being countered by novel defense strategies. The Pentagon envisions a war in the heavens, but can it defend the ultimate high ground? You bet! Witness the experimental idea of setting up a decoy network separate from your real one to fool intruders as they try to fool you.

Deception Network

This so-called deception network is envisioned as more than just a single server set up to be a "honeypot," where hackers may break in, find a dead-end, and have their activities recorded with an eye toward prosecution. Rather, the decoy net is an entire fake network, complete with host computers on a LAN with simulated traffic, to convince hackers for as long as possible that it's real.

Experts debate whether such nets will be worth the effort, but agree they can be a way to slow hackers long enough to sort the curious from the truly destructive "snuff." A group calling itself the Honeynet Project has quietly begun testing decoy networks on the Internet.

The Honeynet Project is not intended to prosecute intruders who haplessly wander into their elaborate decoys, but to study hacker responses in depth to devise the best decoy defenses. Other decoy networks slow intruders with an eye toward collecting evidence to prosecute them. To collect evidence, you need to divert the hacker to a deception network. The idea is to feed back information about what hackers do to a kind of "deception central" for network administrators. The time the hackers are dealing with a deception environment is time they're not in your network.

It is possible to create a deception network that has the same IP network address as your real network. Deception nets carry obvious administrative burdens, such as the need to generate realistic traffic to fool a hacker and maintain a network no one really uses.

NOTE

There is a risk that administrators will lose track of what's real and what's not.

These deception techniques have doubters. It's not clear yet if you can fool a lot of people with this deterrent. Meanwhile, hackers continue to learn new tricks. It's pretty nasty stuff. For very sensitive networks, you may want to activate port-level security on your switches.

Many tools that let hackers carry out surveillance are now Web-based. Why Web-based? It's easy. No complicated downloads or zip files. They can hack from anywhere, and it's anonymous. Although a talented few among hackers actually make attack tools, many of these tools today are freeware and they're posted on dozens of techie sites, not the secret underground. The tool, which involves launching an attack to determine operating system weakness, was given solely to vendors, but somehow ended up posted on the Packetstorm site in its depository for tools. In the wrong hands this tool is dangerous, but that version isn't as dangerous as other versions that will be released.

The New IW Space Race

The war was not going well. Serbian forces were sowing terror across Kosovo. NATO pilots squinting through clouds could do little to stop them. Errant NATO bombs had killed dozens of civilians and shaken support for the alliance. Then the Pentagon saw it had another problem. A Colorado outfit, called Space Imaging, was about to launch a picture-taking satellite with clarity nearly as good as that of U.S. spy satellites. The company could have sold photos of NATO air bases or troop encampments to, for instance, Serbian operatives. That had to be stopped. But how?

The brass canvassed its experts for recommendations. The U.S.-licensed firm could simply be ordered not to take pictures over a broad swath of Europe. A similar ban could be issued for a few other key areas, such as northern Albania. In the end, however, no order was issued. A malfunction sent Space Imaging's satellite plunging into the Pacific Ocean 30 minutes after it lifted off.

Fortune may not be so kind next time. Space Imaging launched another satellite and started selling pictures from it. Several other companies are right behind it. Before too long, an international bazaar for high-quality satellite imagery will be open for business, and potential foes are making headway with their own satellite capabilities. There's a new proliferation of space-based capabilities. Plus, the United States' Cold War–era capabilities have atrophied.

That's pushing the Pentagon into a whole new kind of warfare. In the future, the U.S. military will be responsible for countering space systems and services used for hostile purposes. That's a nice way of saying the Pentagon needs to be prepared to defend the ultimate high ground by attacking hostile satellites. The new policy also directs the Space Command to start developing tactics and doctrine for conducting warfare in the heavens. It must also come up with plans for deploying space-based lasers or other weapons that could be used against targets anywhere on Earth or above it. If the United States ultimately deploys such weaponry, not only would it break one of the great taboos of the past 53 years, but it could also transform the way America structures its military and fights wars.

Aggressive "space control," as the military calls its quest for dominance in the sky, could backfire. The military view is that it would be the neatest thing in the world to have a death ray in space, but will deploying it lead to a war with somebody?

Very possibly, some critics say. Developing space weapons would be a mistake of historic proportions that would trigger an arms race in space. Imagine scenarios in which other nations follow the U.S. example and scramble to launch their own space weapons while frantic generals, unable to tell exactly who has put what into orbit, plead for extravagant countermeasures. In Pentagon war games, just trying to defend U.S. satellites causes problems. If you defend the satellite, you often widen the war. The activity ends up being the problem and not the solution.

IW WEAPONS OF THE FUTURE

Now let's look at some really "far out" IW arsenals of the future: spy dust and tiny mechanical robots. Let's look first at spies the size of a mote of dust. This will be followed by tiny robotic insects that may soon serve as military scouts.

Spy Dust Balls

"If only these walls could talk" may not be an idle plea much longer. Kris Pister, expectant father of an invention he calls "smart dust," thinks that in a few years almost anything, from a wall to a mote floating in the air, may have a story to tell (see sidebar, “A Dusty Future”). Thousands of these gossipy particles, each a tiny bundle of electronic brains, laser communications system, power supply, sensors, and even a propulsion system, could lurk all around, almost undetectable. One or more of the remote sensors would fit inside the letter “O.”

A DUSTY FUTURE

Scientists recently set up a network of small, wireless sensors called motes that detect birds as well as measure temperature, humidity, and barometric pressure. The battery-powered devices transmit their data by radio link to a solar-powered base station and then to the Internet. You can literally be anywhere in the world and know what’s going on.

Thanks to this new technology, many scientists are getting the chance to observe what was previously unobservable. Just as MRI technology revolutionized the ability to peer inside the body, the new networks are expected to shed much-needed light on planetary problems like climate change and how pollutants move through the environment. Other researchers are testing the devices for modeling earthquake damage and monitoring everything from vehicle movements in war zones to water use in agricultural fields.

However, while smart dust is generating excitement, some people already are concerned about the dark side of what will undoubtedly be its expanded presence on the landscape. It’s a very intrusive technology and could be abused.

Sensors and computer chips have long been embedded in consumer products, whether cars or refrigerators. What’s new is that because motes are wireless and battery-powered, they can be used in previously hard-to-access places and moved around at will. Before the technology takes off, motes may have to get smaller—currently, prototypes are the size of matchboxes. The devices also will have to become cheaper, more reliable, and more energy efficient, but there’s little doubt that they could serve as ubiquitous information collectors. These networks of tiny communicating computers could even function as a new kind of Internet that, by merging with the physical world, would allow us to query almost anything—buildings, roads, rivers—for information.

The technology was jump-started in 1998, when Kris Pister, then an engineer at the University of California-Berkeley and now CEO of Dust Inc., got funding from the DoD’s Defense Advanced Research Projects Agency (DARPA) to develop tiny, intelligent sensing devices. He had no idea what the applications would be and never in his wildest dreams expected it would lead where it has. The initial challenge was to miniaturize the components, including the sensors, radio transmitters, batteries, and computer hardware. Programming the devices also was tricky because they

→

needed to be both smart and energy efficient. Recently, scientists solved this problem by designing software that enabled the motes to sleep most of the time, yet wake up regularly to take readings and communicate. The scientists didn't want lots of people to have to baby-sit the motes.

Indeed, an early test in March 2001 showed just how independent the devices could be. At a military base in Twentynine Palms, California, Pister and his team dropped six motes from an airplane along a road. As soon as they hit the ground, they organized themselves into a network and began sensing the magnetic field around them. When that changed as a vehicle drove by, the motes cooperated to calculate its speed and direction, later transmitting the data to a laptop at a nearby base camp.

Now, several companies make prototypes with customized sensors that are showing great promise in field tests. For instance, in 2003, scientists deployed motes made by Intel to measure sunlight, temperature, and humidity in a half-dozen redwood trees in a botanical garden. In addition to eliminating miles of airing (moving out) and reducing the cost of the experiments 10-fold, the motes will give scientists the first 3-D view of the redwood forest microclimate. Recently, scientists packed up the motes and moved them to a remote natural grove. Their goal is to better understand how the loss and fragmentation of redwood forests affect local climate and water resources. In an even more ambitious study of ecosystems, UCLA's Center for Embedded Network Sensing (CENS) is setting up a network with a couple hundred devices in a forested 40-acre reserve near Palm Springs.

Motes are poised to become practical tools for protecting and managing all sorts of resources. For instance, CENS will test motes to monitor an alfalfa field to see how well the plants dissipate high-nitrate wastewater. In 2003, a vineyard in British Columbia deployed a network of 65 motes to closely track temperature fluctuations on its slopes. One aim is to determine when temperatures are perfect for picking grapes to make a late-harvest wine known as ice wine.

While the applications of wireless sensor networks seem endless, the first field tests have revealed shortcomings, which companies are working hard to address. Generally, the motes have needed more-robust packaging to survive rough treatment, curious animals, and frigid weather. At times the radios have been as fickle as cell phones in their signaling and reception.

Still, the biggest challenge may be dealing with the crushing load of information in smart dust. For instance, the Embedded Collaborative Computing Area at the Palo Alto Research Center in California, is trying to reduce the volume of incoming data by training the motes to pay attention only to what's important in the surrounding environment. Others are trying to ensure that the data is accurate and secure—a crucial step if motes are ever to be used for, for example, monitoring a city for signs of bioterrorism.

→

As motes are deployed more and more widely, the potential for the misuse of the information they collect can only grow. Scientists at Berkeley's Center for Information Technology Research in the Interest of Society are already looking at how laws might be updated to protect the privacy of individuals whose comings and goings, for instance, may one day be tracked by motes. Scientists don't think it will be difficult to draw the lines, but they do need to ask, How far do we let this go? It's a question far removed from observing seabirds on a wind-swept island.

Pister exemplifies the surging confidence of the leaders in a new field called MEMS (microelectrical and mechanical systems). The idea is to build complex gadgets so small one needs a microscope to see the parts, using fabrication methods invented by the electronics industry for making silicon chips. He talks big and earnestly, even though the best his prototypes (an undustlike inch or so across) can do is exchange laser signals with a counterpart on a tennis court visible 900 yards away through his fifth-floor office window at the University of California-Berkeley—but that's enough to show that the components work. Miniaturizing them is well within current technology.

Tracking Tots

Cheap, dispersed sensors may tell farmers the exact condition of their acreage; manufacturers, the precise humidity and temperature history of their raw materials; parents, the locations and conditions of their small children all the time. Climate-control systems in buildings would know exactly where it is too cold, humid, hot, or drafty. In five years, smart dust could be linked by satellite. Eventually, you could log on to readings from smart dust almost anywhere. One dream of Pister is to explore outer space with smart dust. NASA could scatter smart dust sensors into the Martian atmosphere and they'd settle all over the planet (like in the recent movie *Red Planet*).

They could also be used as tiny spies. In 1992, as a new associate professor at the University of California-Los Angeles, Pister attended a Rand Corp. workshop in Santa Monica sponsored by the DARPA. The topic was miniaturization of novel battlefield surveillance methods. The question was whether tiny electronic sensors could be scattered in contested territory to relay vital information back to commanders. You could find out, for example, if a tank had gone by or whether there was anthrax in the air. The concept sent his imagination racing.

Poppy Seeds

Pister coined the label *smart dust* in 1996 and produced the first complete smart-dust particle in mid-2002, about 1 millimeter on a side, or roughly between a poppy seed and a grape seed in size. None of the unit's components seems to present major fabrication obstacles. Before building the first fully small versions, however, the team wants to be sure it can get oversize prototypes to work. One of the students is working on a variant that will sport a thin, winglike extension, like that of a maple seed, so that a modest breeze will keep it aloft. Another student is designing a solid rocket micromotor, visible with a good magnifying glass, carved out of silicon. If a smart dust particle detects a tank going by, it could hop up and hitch a ride like a little spy. Some smart dust may be equipped with solar cells for power. Others might alight on vibrating machinery to soak up energy from the motion or charge batteries off electromagnetic pulsations leaking from power lines. Sensors, at first, would be simple (such as for temperature, humidity, a few targeted chemicals, etc.), but eventually microphones and camera systems should be possible.

Pister tells the grad students and postdocs in the engineering school's smart dust group that above all, they must have a passion for new ideas and teamwork. He warns them against giving in to the "dark side" (Big Brother), against becoming stealth researchers whose distrust of others makes them, in his words, roach motels for information. Love of freely flowing communication is appropriate from a man who expects a tomorrow suffused with tiny snoops. He knows his ideas may occasionally serve nefarious ends, invading privacy or monitoring citizens of authoritarian governments. His reply to nervous objections is simple. "Information is good, and information flow reinforces democracy and not tyranny." Well, maybe.

Mechanical Dragonflies

The military calls it "situational awareness": the ability to detect how many hostile tanks await in the next valley or if bombed-out buildings are filled with snipers. It is an advantage that has proved difficult to attain: spies, satellites, and U-2s have all failed to keep commanders from blundering into ambushes and mismatches. The worst thing is just not knowing where the enemy is. It's having the sense that somebody's out there trying to get you but having no idea of where the enemy might be.

Military researchers are working to free future American troops from the terror of the unknown. The researchers envision tomorrow's soldiers coming to a hill, halting, and reaching into their packs for cigar-shaped tubes. From every tube emerges a robotic spider, or a robotic dragonfly, each no longer than 3 inches. Equipped with cameras or acoustic sensors, the mechanical insects range forward and provide data on the hazards that lie in wait on the other side: the number of machine gun nests and the position of artillery.

Backed by $7.7 million from DARPA, military researchers are designing such insect-inspired spies. Recently, the researchers built their first crawling bug prototypes, and they aim to perfect the design within two years. Insect-shaped "micro aerial vehicles" are next on the slate. Along with providing the military with state-of-the-art scouts, the researchers hope their project alters the way engineers approach the long-vexing problem of robotic locomotion.

In most robotic systems today, people think that if you want to move one joint, then you need to attach a motor at that joint. That makes for large, bulky, energy-hog robots. It also reduces robots to the ranks of expensive toys. Motors are only about 80% efficient in turning electrical power into movement, so, although robots may impress with their futuristic looks, most motor-driven devices have ranges limited to only a few dozen yards, rendering them useless for practical applications.

In the initial design, piezoelectric ceramics—thin, ceramic-coated metal wafers that bend when an electrical current is applied to their surfaces—were proposed. Such materials already are used commercially to make silent pagers vibrate or to make zoom lenses move strips (built from lead, zirconium, and titanium) that are sandwiched together, a structure known as a bimorph actuator. When charged, one half of the actuator expands while the other contracts, causing it to curve. When the brief energy pulse ends, the structure snaps back to its original form and then can begin the cycle anew. The researchers attached titanium legs to these vibrating strips. Vibration is translated into motion, as the crawler takes 2-millimeter-long forward strides in response to each oscillation.

Because piezoelectrics require only occasional energy boosts to keep up the vibration, the bugs promise to be up to 70% more energy efficient than traditional robots. If you're in a weight room and you lift 100 pounds up and down 10 times, that takes a lot of energy from a person (illustrating the principle behind the design). The same work could more easily be accomplished by hooking that weight to a spring on the ceiling, then displacing it a bit and letting it bounce up and down by itself. Another common analogy is a child on a swing; once in motion, very little pumping action is required to keep moving. The bugs' energy efficiency should give them ranges of almost 600 yards and allow them enough juice to carry such intelligence-oriented payloads as chip-size infrared detectors and quarter-size video cameras.

Natural Efficiency

The engineers' decision to model their robots after bugs was a natural choice: biological systems are far more energy efficient than anything cooked up in the laboratory. Most things biological sort of oscillate as they walk. If you look at humans walking and the way our legs act as pendulums off our hips and swing back and forth, that's a cyclic motion. They were also impressed by the shape of daddy longlegs, whose low-slung bodies and inverted-V legs create a stable configuration—important for robots that will have to scamper across uneven, sometimes treacherous terrain. Additional hardiness comes from the solid-state legs, which are free of bearings, rods, or shafts that could get jammed by pebbles or dust. They probably won't survive being stomped on, but short of that they're pretty tough. They could actually survive four-story falls.

Before the bugs can be unleashed on the battlefield, however, a few major hurdles remain. Chief among them is a power problem; though the robots will require around 60 volts to start vibrating, the watch-size batteries being considered can provide only 3 to 6 volts. To get the bugs moving without the aid of chargers, circuitry must be developed to amplify the current, and it must be small enough to fit the 2-by-3/4-inch bugs. Still, the design's voltage requirement is impressively low; rival efforts to create locomotive robots of comparable size have needed well over 1,000 volts.

Another lingering question is how a robotic swarm can be controlled. With thousands of bugs roving at once, commanding each individual unit would be close to impossible, so a battalion leader, outfitted with a remote control, would only have to control a "mother ship," an insect at the fore that would then relay instructions to other members of the swarm. In the event of the mother ship's destruction, the leadership role could be shifted to a surviving robot. The exact details of this control, however, have yet to be worked out.

DARPA officials and the researchers are optimistic that the kinks can be worked out and that assembly-line production of the bugs is nearing. Along with the crawling prototype, the researchers have already managed to construct a piezoelectrically actuated thorax for the flier. Once all design issues are resolved, the researchers believe, the insects could cost as little as $7 per unit. The required metals are readily available, and the bimorph strips and legs can be cheaply pressed from large sheets.

The low price makes the insects potential candidates for a variety of uses, including delivering lethal toxins on the battlefield or aiding police SWAT teams. Perhaps 40,000 of the mechanical creatures could be dropped on the Martian surface to probe the nooks and crannies Pathfinder missed. Those missions are far distant, though; the bugs' first and foremost duty will be to give American troops an upper hand and to save them from stumbling into situations too perilous to survive.

Finally, let's look at how machines the size of molecules are creating the next industrial revolution in IW.

NANOTECHNOLOGY

In 2000, a group of scientists from the University of Michigan's Center for Biologic Nanotechnology traveled to the U.S. Army's Dugway Proving Ground in Utah. The purpose of their visit was to demonstrate the power of "nano-bombs." These munitions don't exactly go "Kaboom!" They're molecular-size droplets, roughly 1/5,000 the head of a pin, designed to blow up various microscopic enemies of mankind, including the spores containing the deadly biological warfare agent anthrax.

The military's interest in nano-bombs is obvious. In the test, the devices achieved a remarkable 100% success rate, proving their unrivaled effectiveness as a potential defense against anthrax attacks. Their civilian applications are also staggering. For example, just by adjusting the bombs' ratio of soybean oil, solvents, detergents, and water, researchers can program them to kill the bugs that cause influenza and herpes. Indeed, the Michigan team is now making new, smarter nanobombs so selective that they can attack *E. coli*, salmonella, or listeria before they can reach the intestine.

If you're a fan of science fiction, you've no doubt encountered the term *nanotechnology*. Over the past 23 years, scores of novels and movies have explored the implications of mankind's learning to build devices the size of molecules. In a 1999 episode of *The X-Files* titled "S. R. 819," nanotechnology even entered the banal world of Washington trade politics, with various nefarious forces conspiring to pass a Senate resolution that would permit the export of lethal "nanites" to rogue nations.

Since 1999, a series of breakthroughs have transformed nanotech from sci-fi fantasy into a real-world applied science and, in the process, inspired huge investments by business, academia, and government. In industries as diverse as health care, computers, chemicals, and aerospace, nanotech is overhauling production techniques, resulting in new and improved products—some of which may already be in your home or workplace.

Silicon Fingers

Meanwhile, nearly every week, corporate and academic labs report advances in nanotech with broad commercial and medical implications. In 2000, for example, IBM announced it had figured out a way to use DNA to power a primitive robot with working silicon fingers 1/50 as thick as human hair. Within a decade or so, such devices may be able to track down and destroy cancer cells. At Cornell University, researchers have developed a molecule-sized motor, built out of a combination of organic and inorganic components, which some dub nanotech's "Model T." In tests announced in 2003, the machine's rotor spun for 120 minutes at 6 to 7 revolutions per second. When further developed, such motors will be able to pump fluids, open and close valves, and power a wide range of nanoscale devices.

These inventions and products are just the beginning of what many observers predict will be a new industrial revolution fostered by man's growing prowess at manipulating matter one atom, or molecule, at a time. Because of nanotech, all of us will see more change in our civilization in the next 30 years than we did during all of the 20th century.

NOTE

Nanotech takes its name from the nanometer, a unit of measurement just one billionth of a meter long.

Imagine the possibilities. Materials with 10 times the strength of steel and only a small fraction of the weight. Shrinking all the information housed at the Library of Congress into a device the size of a sugar cube. Or detecting cancerous tumors when they are only a few cells in size.

To build such objects, engineers employ a wide range of techniques, borrowed from bioengineering, chemistry, and molecular engineering. Such feats include imitating the workings of the body, where DNA not only programs cells to replicate themselves but also instructs them how to assemble individual molecules into new materials such as hair or milk. In other words, many nanotech structures build themselves.

Atom by Atom

The inspiration for nanotech goes back to a 1959 speech by the late physicist Richard Feynman, titled "There's Plenty of Room at the Bottom." Feynman, then a professor at the California Institute of Technology, proposed a novel concept to his colleagues. Starting in the Stone Age, all human technology, from sharpening arrowheads to etching silicon chips, has involved whittling or fusing billions of atoms at a time into useful forms. What if we were to take another approach, Feynman asked, by starting with individual molecules, or even atoms, and assembling them one by one to meet our needs? The principles of physics, as far as Feynman could see, did not speak against the possibility of maneuvering things atom by atom.

Four decades later, Chad Mirkin, a chemistry professor at Northwestern University's $45-million nanotech center, used a nanoscale device to etch most of Feynman's speech onto a surface the size of about 10 tobacco smoke particles—a feat that Feynman would no doubt have taken as vindication. The course science took to achieve such levels of finesse has not always been straightforward. Nor has it been lacking in controversy.

Indeed, some scientists are alarmed by nanotechnology's rapid progress. In 2000, the chief scientist at Sun Microsystems created a stir when he warned that in the wrong hands, nanotech could be more destructive than nuclear weapons. Influenced by the work of Eric Drexler, an early and controversial nanotechnology theoretician, the scientist predicted that trillions of self-replicating nanorobots could one day spin out of control, literally reducing the earth's entire biomass to gray goo.

Most researchers in the field don't share that type of concern. They are compelled to keep going. Researchers are knocking on the door of creating new living things, new hybrids of robotics and biology. Some may be pretty scary, but they have to keep going.

The early payoffs have already arrived. Computer makers, for example, use nanotechnology to build "read heads," a key component in the $45-billion-a-year hard disk drive market, which vastly improve the speed at which computers can scan data. Another familiar product, Dr. Scholl's brand antifungal spray, contains nanoscale zinc oxide particles—produced by a company called Nanophase Technologies—that make aerosol cans less likely to clog. Nanoparticles also help make car and floor waxes that are harder and more durable and eyeglasses that are less likely to scratch. As these examples show, one huge advantage of nanotech is its ability to create materials with novel properties not found in nature or obtainable through conventional chemistry.

What accounts for the sudden acceleration of nanotechnology? A key breakthrough came in 1990, when researchers at IBM's Almaden Research Center succeeded in rearranging individual atoms at will. Using a device known as a scanning probe microscope, the team slowly moved 35 atoms to spell the three-letter IBM logo, thus proving Feynman right. The entire logo measured less than three nanometers.

Soon, scientists were not only manipulating individual atoms but also "spray painting" with them. Using a tool known as a molecular beam epitaxy, scientists have learned to create ultrafine films of specialized crystals, built up one molecular layer at a time. This is the technology used today to build read-head components for computer hard drives.

One quality of such films, which are known as giant magnetoresistant materials, or GMRs, is that their electrical resistance changes drastically in the presence of a magnetic field. Because of this sensitivity, hard disk drives that use GMRs can read very tightly packed data and do so with extreme speed. In a few years, scientists are expected to produce memory chips built out of GMR material that can preserve 100 megabits of data without using electricity. Eventually, such chips may become so powerful that they will simply replace hard drives, thereby vastly increasing the speed at which computers can retrieve data.

Natural Motion

The next stage in the development of nanotechnology borrows a page from nature. Building a supercomputer no bigger than a speck of dust might seem an impossible task, until one realizes that evolution solved such problems more than a billion years ago. Living cells contain all sorts of nanoscale motors made of proteins that perform myriad mechanical and chemical functions, from muscle contraction to photosynthesis. In some instances, such motors may be re-engineered, or imitated, to produce products and processes useful to humans.

Animals such as the abalone, for example, have cellular motors that combine the crumbly substance found in schoolroom chalk with a "mortar" of proteins and carbohydrates to create elaborate, nano-structured shells so strong they can't be shattered by a hammer. Using a combination of biotechnology and molecular engineering, humans are now on the verge of being able to replicate or adapt such motors to suit their own purposes.

How are these biologically inspired machines constructed? Often, they construct themselves, manifesting a phenomenon of nature known as self-assembly.

The macromolecules of such biological machines have exactly the right shape and chemical-binding preferences to ensure that, when they combine, they will snap together in predesigned ways. For example, the two strands that make up DNA's double helix match each other exactly, which means that if they are separated in a complex chemical mixture, they are still able to find each other easily.

This phenomenon is potentially very useful for fabricating nanoscale products. For instance, in 1999, a team of German scientists attached building materials such as gold spheres to individual strands of DNA and then watched as the strands found each other and bound together the components they carried, creating a wholly new material.

Similarly, the 1996 Nobel Prize in chemistry went to a team of scientists for their work with "nanotubes"—a formation of self-assembling carbon atoms about 1/50,000 the width of a human hair. Scientists expect that when they succeed in weaving nanotubes into larger strands, the resulting material will be 100 times stronger than steel, conduct electricity better than copper, and conduct heat better than diamond. Membranes of such fibers should lead to rechargeable batteries many times stronger, and smaller, than today's.

In 2000, a team of IBM scientists announced that they had used self-assembly principles to create a new class of magnetic materials that could one day allow computer hard disks and other data-storage systems to store more than 100 times more data than today's products. Specifically, the researchers discovered certain chemical reactions that cause tiny magnetic particles, each uniformly containing only a few thousand atoms, to self-assemble into well-ordered arrays, with each particle separated from its neighbors by the same preset distance.

Other scientists have discovered important new self-assembling entities by accident. In 1996, Samuel Stupp, a professor at Northwestern University, was in his lab trying to develop new forms of polymer when he inadvertently came upon "nanomushrooms." He saw the potential right away. The molecules he had been experimenting with had spontaneously grouped themselves into supramolecular clusters shaped like mushrooms. Soon afterward, Stupp discovered, again accidentally, that he could easily program these supramolecules to form film that behaves like Scotch tape.

Meanwhile, researchers at UCLA and Hewlett-Packard have laid the groundwork for the world's first molecular computer. Eventually, the researchers hope to build memory chips smaller than a bacterium. Such an achievement is essential if computing power is to continue doubling every 18 to 24 months, as it has for the past four decades. This is because the more densely packed the transistors on a chip become, the faster it can process, and we are approaching the natural limit to how small transistors can be fabricated out of silicon.

Future Phenomena

Where will it all end? Many futurists have speculated that nanotech will fundamentally change the human condition over the next generation. Swarms of programmable particles, sometimes referred to as "utility fog," will assemble themselves on command. The result could be a bottle of young wine molecularly engineered to taste as if it had aged for decades or a faithful biomechanical dog with an on/off switch.

Meanwhile, new, superstrong, lightweight nanomaterials could make space travel cheap and easy and maybe even worth the bother, if, as some scientists predict, nanotech can be used to create an Earth-like atmosphere on Mars. Space colonization could well be necessary if the new science of "nanomedicine" extends life indefinitely, manufacturing new cells, molecule by molecule, whenever old cells wear out. It all seems hard to imagine, yet nanotech has already produced enough small wonders to make such big ideas seem plausible, if not alarming—at least to the high priests of science and the IW military strategists.

SUMMARY

Information technology is being developed by strategic planners both as an offensive battlefield weapon and as a weapon for "logistics attack," as a means to disrupt the civilian infrastructure on which an enemy's military apparatus depends. Technology has already been used effectively by U.S. forces in the Gulf War, in Iraq and in the conflict in Haiti.

However, IW is a double-edged sword. Those countries most capable of waging it are also the ones most vulnerable to it. The increasing dependence on sophisticated information systems brings with it an increased vulnerability to hostile elements and terrorists.

Conclusions

- Even though the anticipated national security threats of the coming decades involve less-developed countries, the Collaborative Virtual Workspace (CVW) threat and other methods of intrusion and disruption are not necessarily beyond their reach. CVW is a collaboration software environment that provides a virtual building where teams can communicate, collaborate, and share information, regardless of their geographic location.
- Opportunities to deceive and confuse through an elaborate misinformation scheme along a myriad of information paths are available to anyone.
- The IW arsenal of the future provides a new avenue to employ deception techniques through the use of multiple paths that create the perception and validation of truth.

- There exists the prospect of an intelligence analyst manipulating an adversary's command-and-control system so that reality is distorted.
- Tomorrow's soldier will depend more than ever on the very well-known and trusted factors of mobility.
- Imagine a scenario depicting a "left hook" in the Iranian desert that fails because the systems in use were successfully attacked by CVW, or some other intrusion method, with the resulting disruption putting U.S. troops in a flailing posture—facing the unknown and losing confidence in their operation.
- One thing is sure. An Iranian "left hook" will be difficult to repeat.
- One can assume that Iran, and others, will exploit the GPS to their own advantage. The IW arsenal is coming of age.
- World War II set the stage, but only with today's technology can we expect action in this sphere of warfare on a grand scale.
- The necessity to prevent irresponsible groups and individuals from getting access to nanotechnological manufacturing capability will be a prime concern in the near future.
- The chapter has shown how this quest for containment has shaped many aspects of society, most notably via the institution of a global surveillance network.

An Agenda for Action

In the United States, where the threat is most immediately recognized, debate is currently going on to decide what part government can and should play in protecting civilian networks. On the one hand, the civilian networks are controlled by private interest groups, some of them internationally owned. Government regulation would seem to be interference or even repression. On the other hand, the vulnerability and ease of manipulation of some networks are weak links in modern society, and their exploitation by hostile elements threatens all elements of society, not just the direct controllers of the networks. One solution is to require organizations with a dependence on sensitive information technology to fulfill certain security criteria before being issued a government license. Something like this has been done in Israel already, with the legislation of the "computer laws" of 1994.

The U.S. government needs to set an agenda for action that goes beyond the work already done in preparation for defending against the IW arsenal of the future. Action steps should include, but not be limited to the 12 areas shown in Table F17.1 in Appendix F.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Even though the anticipated national security threats of the coming decades involve less-developed countries, the CVW threat and other methods of intrusion and disruption are necessarily beyond their reach.
2. True or False? Opportunities to deceive and confuse through an elaborate misinformation scheme along a myriad of information paths are not available to anyone.
3. True or False? The IW arsenal of the future provides an old avenue to employ deception techniques through the use of multiple paths that create the perception and validation of truth.
4. True or False? Tomorrow's soldier will depend more than ever on the very well-known and trusted factors of mobility.
5. True or False? One can assume that Iran, and others, will exploit the GPS to their own advantage.

Multiple Choice

1. Among the current possible offensive weapons are the following, except:
   A. Computer viruses, which could be fed into an enemy's computers either remotely or by "mercenary" technicians
   B. Nuclear bombs, another type of virus which can lie dormant for years, until, upon receiving a particular signal, would wake up and begin attacking the host system
   C. "Chipping," a plan (originally proposed by the CIA, according to some sources) to slip booby-trapped computer chips into critical systems sold by foreign contractors to potentially hostile third parties (or recalcitrant allies?)
   D. Worms, whose purpose is to self-replicate ad infinitum, thus eating up a system's resources
   E. Trojan horses, malevolent code inserted into legitimate programming to perform a disguised function
2. The Privacy Foundation at the University of Denver conducts research into communications technologies and provides the public with tools to maintain privacy in the Information Age. You can read the Foundation's report and commentary on email wiretaps. The report cites the following possible uses for this security breach, except:

A. The wiretaps can provide the ability to monitor the path of a confidential email message and the written comments attached.
B. In a business negotiation conducted via email, one side can learn inside information from the other side as the proposal is discussed through the recipient company's external email system.
C. A bugged email message can capture thousands of email addresses as the forwarded message is sent around the world.
D. Commercial entities, particularly those based offshore, may seek to offer email wiretapping as a service.

3. Computers used in data processing systems are all potentially vulnerable to the EMP effect, such as the following, except:

A. Open source intelligence
B. Communications systems
C. Displays
D. Industrial control applications

4. The electromagnetic device will be detonated by the missile's onboard fusing system. In a cruise missile, this will be tied to the following, except:

A. Navigation system
B. Antishipping missile
C. Internet protocol
D. Radar seeker
E. Air-to-air missile, the proximity fusing system

5. The necessity to prevent irresponsible groups and individuals from getting access to nanotechnological manufacturing capability is a prime concern in:

A. The near future
B. The past
C. Traditional psychological operations or deception operations
D. Covert media manipulation
E. Clandestine human intelligence operations or overt research operations

Exercise

In a breach of contract case it was decided on a Friday to use a computer forensics specialist (CFS) to recover company emails. The attorney needed all the plaintiff company's emails and attachments over a seven month time frame, meeting keyword and time/date criteria immediately. Over 1,090,000 total emails met the criteria. The emails and system were password protected and the passwords were not available. How was the CFS able to go about recovering the email?

HANDS-ON PROJECTS

An examiner at a major financial institution in Chicago successfully previewed two drives in Asia connected to the company-wide area network. The drives were previewed in less than an hour after management determined that the investigation was necessary and that time was of the essence. The preview process revealed that one of the drives contained highly relevant information and the drive was promptly acquired for further forensic analysis in Chicago. How did the CFS team (CFST) go about conducting their investigation?

Case Project

A large government agency used a CFS and a high-speed network connection to image a drive on its wide area network (WAN) located approximately 11,000 miles (17,600 km) away. How did the CFS go about conducting the investigation?

Optional Team Case Project

Law enforcement investigators arrived at a company site to collect computer evidence from a server. The company was not the perpetrator of the investigated crime, but apparently did possess important evidence that resided on a mission-critical server that could not be taken off-line. How was the CFS able to go about conducting the investigation?

REFERENCES

[1] Vacca, John R., *The Cabling Handbook*, 2nd ed., Prentice Hall, New York, 2001.

[2] Vacca, John R., *i-mode Crash Course*, McGraw-Hill, New York, 2002.

[3] Vacca, John R., *Satellite Encryption*, Academic Press, New York, 1999.

[4] Vacca, John R., *The World's 20 Greatest Unsolved Problems*, Prentice Hall, New York, 2004.

[5] Rowling, J. K., *Harry Potter and the Chamber of Secrets*, Scholastic Trade, New York, 1999.

This page intentionally left blank

18 Surveillance Tools for Information Warfare of the Future

Wireless systems [1] capable of monitoring vehicles and people all over the planet (basically everything) are leaving businesses and the military aglow with new possibilities—and some privacy advocates deeply concerned. Companies seeking to tap the commercial potential of these technologies are installing wireless location systems in vehicles, hand-held computers, cellphones—even watchbands. Scientists have developed a chip that can be inserted beneath the skin, so that a person's location can be pinpointed anywhere.

For example, the owner of a small company in Dallas that installs automobile alarms uses a wireless tracking service to monitor his fleet of six Dodge Dakota pickup trucks, and the equipment alerted him recently when one of his trucks turned up in the parking lot of the Million Dollar Saloon, a strip club. When he signed up for this service, he told his guys, "Big Brother's keeping an eye on you, and I'm Big Brother." After he fired that one fellow, you bet they all believed him.

These technologies have become one of the fastest-growing areas of the wireless communications industry. The market for location-based services is already estimated at nearly $1 billion and is forecast to approach $9 billion by 2007.

MONITORING EVERYTHING

A federal effort to make it easier to pinpoint the location of people making emergency 911 calls from mobile phones means that cell phones sold in the United States are now equipped with advanced wireless tracking technology. Various plans already under way include alerting cell-phone users when they approach a nearby McDonald's, telling them which items are on sale, and sending updates to travelers about hotel vacancies or nearby restaurants with available tables. One Florida company wants to provide parents with wireless watchbands that they can use to keep track of their children.

Although the commercial prospects for wireless location technology may be intriguing, and the social benefits of better mobile 911 service are undisputed, privacy-rights advocates are worried. By allowing location-based services to proliferate, you're opening the door to a new realm of privacy abuses. What if your insurer finds out you're into rock climbing or late-night carousing in the red-light district? What if your employer knows you're being treated for AIDS at a local clinic? The potential is there for inferences to be drawn about you based on knowledge of your whereabouts.

Until recently, location-based services belonged more in the realm of science fiction than commerce. Although satellite-based global positioning system (GPS) technology has been commercially available for some time for airplanes, boats, cars, and hikers, companies have only recently begun manufacturing GPS chips that can be embedded in wireless communications devices [1]. GPS uses satellite signals to determine geographic coordinates that indicate where the person with the receiving device is situated. GPS monitoring technology will be discussed in much greater detail later in the chapter.

Real-life improvements in the technology have come largely from research initiatives by start-up companies in the United States, Canada, and Europe as well as from large companies like IBM, which recently formed a "pervasive computing" division to focus on wireless technologies such as location-based services.

Location technology is a natural extension of e-business. It's no surprise that a whole new ecology of small companies has formed to focus on making it all more precise. For instance, Peter Zhou, the chief scientist for Applied Digital Solutions, a company in Palm Beach, Florida, helped create a chip called Digital Angel that could be implanted beneath human skin, enabling his company to track the location of a person almost anywhere using a combination of satellites and radio technology. After all, he reasoned, wouldn't the whereabouts of an Alzheimer's patient be important to relatives? Wouldn't the government want to keep track of paroled convicts? Wouldn't parents want to know where their children are at 10 P.M., 11 P.M., or any hour of the day?

A review of Digital Angel's commercial potential, though, revealed concern over the possibility of privacy abuses [3]. Professor Zhou altered his plans for Digital Angel, which is about the size of a dime, so that instead of being implanted it could be affixed to a watchband or a belt. Embedding technology in people is too controversial, but that doesn't mean a system capable of tracking people wherever they go won't have great value. Digital Angel is now commercially available.

That Professor Zhou found himself in the middle of the privacy debate is no surprise, given the growing interest in location-based services. Through the use of existing cellular communications technology or the GPS, researchers' ability to track wireless devices more precisely is growing [4].

Some of the world's largest wireless carriers, such as Verizon Wireless, Vodafone of Britain, and NTT DoCoMo of Japan, are promoting the technology, in addition to dozens of small companies in the United States and Europe. The SignalSoft Corporation, based in Boulder, Colorado, develops software that allows tourists and business travelers to use their mobile phones to obtain information on the closest restaurants or hotels in a given city [5]. Meanwhile Cell-Loc Inc., a Canadian company, has already installed a wireless service in Austin, Texas, and in Calgary, Alberta, that, after determining a caller's location, delivers detailed driving directions.

Some companies are even more ambitious. Webraska, a French company that secured $90 million in financing from investors in the United States and Europe, has mapped every urban area in the world and allows these maps to be retrieved in real time on wireless devices.

While businesses around the world seek to improve the quality of location-based services, the biggest impetus behind the advancement of the technology has come from the federal government, through its effort to improve the precision of locating wireless 911 emergency calls. Nearly a third of the 593 million 911 calls made in 2003 came from cell phones, according to the National Emergency Number Association.

With the number of wireless users growing, carriers are now equipping either cell phones or their communications networks with technology that would allow authorities to determine the location of most callers to within 600 feet, compared with current systems that can locate them within about 900 feet. For example, Verizon Wireless and Western Wireless have developed a network-based system that pinpoints the signal on a handset using the existing cellular network to determine the location, whereas other carriers including Sprint PCS, Alltel, and Nextel favor handsets equipped with GPS chips. Supporters of the initiative, called "E-911" for "enhanced 911," expect the technology's precision to be even better than the federally mandated 600-foot radius.

If your cell phone is on while you're driving, you can tell which intersection you're at. Although the E-911 initiative has driven wireless carriers in the United States to improve their location technology, industry groups have started to grapple with privacy issues. The Wireless Advertising Association, a group of carriers, advertising agencies and device manufacturers, encourages companies to allow consumers to choose whether they want location-based services. The association will endorse companies that adhere to the policy.

People are justifiably concerned with the rapidity with which this technology is being deployed. They need to be assured that there is no conspiracy to use this information in an underhanded way.

CYBER SURVEILLANCE

Nicodemo S. Scarfo, the son of Philadelphia's former mob boss, was almost paranoid enough. Scarfo, who has been charged with masterminding a mob-linked loan sharking operation in New Jersey, reportedly used the popular PGP encryption software to shield his computer's secrets from prying eyes and cyber surveillance, but when the feds learned of Scarfo's security measures, they decided to do something that would bypass even the best encryption software. FBI agents sneaked into Scarfo's office in Belleville, New Jersey, on May 10, 1999, and installed a keyboard-sniffing device to record his password when he typed it in.

A seven-page court order authorized the FBI and cooperating local police to break into Scarfo's first-floor Merchant Services of Essex County office as many times as necessary to deploy, maintain, and then remove recovery methods that will capture the necessary key-related information and encrypted files. The case, which is still awaiting trial, appears to be the first in which the U.S. government used such aggressive surveillance techniques during an investigation; some legal observers say the FBI's breaking-and-entering procedures go too far. This case has the potential to establish some very important precedents on this issue.

Scarfo's prosecution comes at a time when the FBI's Carnivore surveillance system (discussed in Chapter 17) is under increasingly heavy fire from privacy groups, and the use of data-scrambling encryption products appears to be growing. Recently, for instance, news leaked out about Yahoo's encrypted Web-based email service it introduced through a deal with Zixit, a Dallas firm.

Scarfo has been charged with supervising an illegal gambling business in violation of state and federal law and using extortionate loan shark tactics, according to a three-count indictment filed in federal court in June 2000. He has pleaded not guilty.

The elder Scarfo, who once ran the Philadelphia mob that also dominated the Atlantic City gambling racket, was imprisoned in 1991 on racketeering charges. The spring 1999 investigation of the younger Scarfo, who is now 38 years old, may be what prompted the previous Clinton administration to recommend changing federal law to allow police to conduct electronic "black bag" jobs.

The idea first publicly surfaced in mid-1999, when the Justice Department proposed legislation that would let police obtain surreptitious warrants and "postpone" notifying the person whose property they entered for 30 days. After vocal objections from civil liberties groups, the administration backed away from the controversial bill. In the final draft of the Cyberspace Electronic Security Act submitted to Congress, the secret-search portions had disappeared.

In January 2000, the previous Clinton administration seemed to change its mind. When criminals such as drug dealers and terrorists use encryption to conceal their communications, law enforcement must be able to respond in a manner that will not thwart an investigation or tip off a suspect.

The feds didn't need a new law—and would instead rely on "general authorities" when asking judges to authorize black bag jobs. A related "secret search" proposal resurfaced in May 2000 in a Senate bankruptcy bill.

In the Scarfo case, the FBI in May 1999 asked for authority to search for and seize encryption-key-related passphrases from his computer as well as install and leave behind software, firmware, or hardware equipment to monitor the inputted data entered on Nicodemo S. Scarfo's computer by recording the key-related information as it is entered. Although the government has refused to release details, this appears to indicate that the FBI was using either a hardware device (inserted into the keyboard or attached to the keyboard cable) or a software program that would quietly run in the background and record keystrokes. With the PGP private key and Scarfo's secret password, the government could then view whatever documents or files he had encrypted and stored on his computer.

Ruling that normal investigative procedures to decrypt the codes and keys necessary to decipher the "factors" encrypted computer file have been tried and have failed, U.S. Magistrate Judge G. Donald Haneke granted the FBI's request. Haneke did not, under federal law, have the authority to grant such an order. The interesting issue is that in those (court) documents the FBI specifically disclaim any reliance on the wiretap statute. If they're on record saying this isn't communications (and it isn't), then that extraordinary authority they have under the wiretap laws does not apply.

If the government is now talking about expanding black bag jobs to every case in which it has an interest and where the subject is using a computer and encryption, the number of break-ins is going to skyrocket. Break-ins are going to become commonplace.

However, the government could successfully argue that break-ins are constitutional. There's nothing in the Constitution that prohibits this kind of anticipatory search. In many respects, it's no different from a wiretap.

A lawyer for Scarfo told the *Philadelphia Inquirer* that he would file a motion challenging the legality of the FBI's black bag job. The FBI's got everything that Scarfo typed on that keyboard (a letter to his lawyer, personal and medical records, legitimate business records, etc.).

Finding a mentally impaired relative, a lost child, or a criminal in a sprawling metropolitan area would be simple if the person were equipped with a personal locator device. The next part of the chapter will take a close look at these information warfare (IW) tracking devices.

THE CYBER FOOTPRINT AND CRIMINAL TRACKING

At 10:00 A.M. one morning in 1999, an elderly woman in Osaka, Japan, became alarmed. Her 74-year-old husband, who suffers from dementia, had left four hours earlier and had not yet returned. She did not panic, but contacted the provider of her personal locator service, Life Service Center. Within a minute, the provider found him on the second floor of a department store, simply by paging a miniature locator device secured to the man's clothes. Forty minutes later, when the man's son arrived at the department store, his father had already left. Fortunately, the service provider continued tracking the elderly man and was able to direct the son to the fourth floor of an Osaka hotel. At 1:10 P.M., the two were reunited. Locus Corp. provided the system that made this possible.

The belief that it should be easy to find anyone, anywhere, at any time with a few pushes of a button has caught on with the advent of the GPS. People imagine a miniature device, attached to one's person, that reports one's whereabouts almost instantaneously. Add the highly practical need to find missing persons promptly, and the personal locator system (PLS) industry is born.

Systems of this nature, whether based on the GPS or some other technology, are being tested throughout the world. Some are already being deployed in Japan. The service alone can be sold by cellular companies, which base it on their wireless infrastructure. Several companies looking into the technology options plan to offer a broad array of services to the public and to businesses.

In Japan, location services are now commercially available to 74% of the nation's population, including Tokyo, Osaka, Kyoto, Yokohama, Nagasaki, and Hiroshima. Initially designed to support the mentally handicapped, personal locator services have expanded to serve children, the elderly, tourist groups, and security patrols, as well. They may also be used to track valuables and recover stolen vehicles. Not surprisingly, service areas coincide with wireless infrastructure deployments, which personal locators have exploited since their beginning in 1998.

In the United States, two further factors encourage the adoption of these geolocation systems. One is the need to effectively monitor offenders on parole and probation. Tagging offenders with locator devices would tighten their supervision and enhance public safety and could even reduce the prison population. The other is the wish to provide wireless callers with enhanced 911 (E-911) emergency services. For land-line telephony, the location of a phone from which a 911 call is made appears automatically on the 911 operator's computer screen. Callers using cellular phones could be anywhere and unlocatable, unless location technology were applied to the wireless telephone system.

Of course, wireless services for locating vehicles have been thwarting car theft and managing fleets of cars since the mid-1980s. Unlike vehicular locators, which are less constrained by size and power, locators borne on the person have to be the size of a pager, and their power output has to be less than 1 W, because they can only carry a small battery that cannot be continuously recharged. Most challenging of all, personal locators have to be able to operate in radio frequency (RF)-shielded areas such as buildings, because people spend a lot of their time indoors.

One PLS Architecture

A PLS is likely to involve a service provider, a location center, and a wireless network. In this setting, three scenarios, each involving a different operating mode, are possible. The person bearing a locator device is either being sought by a subscriber to the service, is seeking help from the subscriber, or, as in the case of a parolee, is having his or her whereabouts monitored continuously.

Consider again the introductory example, but from a system architecture perspective. It is representative of the first scenario, based on the paging mode, wherein the person with the locator device is sought. In this instance, the subscriber calls the service provider, giving the operator there a password and the "wanted" person's identification (user) number (ID). The operator enters the ID into a computer, which transmits it to another computer at the location center. That machine calls the locator device, in effect paging it to establish communication through the PHPS (personal handy phone systems) wireless telephone switching office. Immediately the office forwards the call to the wireless base station nearest the locator.

Once communication is established between the center and the device, the center asks the device for the signal strength data and IDs of any base stations in its vicinity. The locator replies, and from those inputs, plus RF database information on the base stations, the center computes the locator's coordinates. Details of the geolocation technology behind this architecture follow in subsection "Enhanced Signal Strength."

These coordinates are transmitted to the service provider's computer, which displays the missing person's position on a street map for the service operator to report to the subscriber. The user's location is continuously updated on the service provider's map as long as the location center maintains its call connection to the locator device.

In a second scenario, involving the emergency mode, the user of the locator is lost or in dire straits of one sort or another and presses the device's panic button. The locator calls the location center, which computes the user's position and alerts the service provider, which in turn alerts the subscriber to the user's situation.

The system can employ either packet data or voice channel communications. If a data channel is used, the service takes about 8 seconds to obtain a geolocation fix. If a voice channel is used, the wait could last up to 33 seconds because of processing differences between the two channel types.

Several minutes may be added by communication between the service's operator and the subscriber. Such a human interface may be necessary given the complexity of Japanese (as explained in the Japanese example earlier) city-addressing schemes. Otherwise, subscribers using personal computers may obtain the information directly from the computer of either the service provider or location center.

Both the emergency and paging operating modes of PLSs are characterized as intermittent. In addition, a continuous automatic mode, in which the system polls the locator nonstop, is possible. Strictly speaking, the polling is periodic rather than continuous, but the latter term is more common. Of the three locator modes, this last requires the most RF bandwidth and battery power. If it were implemented with a continuous voice call between the system and the locator, the expense would be beyond the reach of most applications. Assuming a minimal cost of 3 cents per minute for airtime, such a connection would cost US $46.59 a day—and also drain the locator battery within a few hours.

Packet data calls between the locator and the rest of the system are far more economical. In the packet version, the locator is likely to be polled every few minutes, exchanging 100 bytes or so with the system in a fraction of a second. Given a 3-minute polling interval and a 1-cent-per-poll cost, the daily cost per locator would be only $4.80.

Most of the time, the locator would be in standby mode, conserving valuable battery charge. Another plus: upcoming third-generation mobile wireless telephony will increase the availability of packet data communications.

Six Technologies

A PLS could use any of several technologies. Among the most common methods are angle and time difference of the signal's arrival, GPS and the more recent assisted GPS, enhanced signal strength, and location fingerprinting.

Signal Direction

The simplest technologyy is based on measuring the direction of a signal received from an RF transmitter at a single point. This can be done by pointing a directional antenna along the line of maximum signal strength. Alternatively, signal direction can be determined from the difference in time of arrival of the incoming signals at different elements of the antenna. A two-element antenna is typically used to cover angles of ±60 degrees. To achieve 360-degree coverage, a six-element antenna can be used.

A single mobile directional antenna can give only the bearing, not the position, of a transmitting object. The single bearing can be combined with other information, such as terrain data, to provide location. Such an antenna is generally used to approach and locate objects up to several kilometers away. A common use of this technique is tracking RF-tagged wildlife. The same basic technique is used by Lo-Jack Corp., of Dedham, Massachusetts, in its system for finding stolen vehicles.

With two directional antennas spaced well apart, however, the position of a transmitting device in a plane can be computed. In this method, also known as the angle of arrival (AOA) method, transmitter position is determined from the known (fixed) position of the receivers' antennas and the angle of arrival of the signals with respect to the antennas.

Angle measurement precision affects the accuracy of positioning calculations, as does the geometry of the transmitting device and receiving antennas. For example, if a transmitter is too near a line drawn between two receiving antennas, its measured position could be off by more than the distance between the antennas. Fortunately, multiple receiver antennas distributed throughout the area of coverage enable the cellular system to select those antennas that introduce the smallest error.

Signal Times of Arrival

Similarly, the time difference of arrival (TDOA) between signals received at the geographically disparate antennas can be used to determine position. Given the speed of light and known transmit and receive times, the distance between the mobile locator and receiver antenna can be calculated.

Accurate clocks are of the essence here, because an error of 1 μs in time corresponds to an error of 300 meters in space. Also, all clocks used must be synchronized, but as synchronizing the mobile locator clock is usually impractical, at least three receiving antennas are required for the calculation. Sometimes the calculations produce ambiguous results, which can be resolved by considering signals received at a fourth antenna. As with the angle of arrival method, the relative positions of receivers and transmitter affect computational errors.

In an alternative time difference scheme, the locator and the antennas reverse roles: the antennas are transmitters and the mobile locator is a receiver. This technique is known as forward link trilateration (FLT). This is relatively simple to implement in some code-division multiple access (CDMA) wireless systems, where the TDOA can be determined from the phase difference between pseudorandom noise code sequences of 0s and 1s transmitted from two antennas.

Global Positioning System

As previously explained, a GPS relies on a constellation of 24 satellites. It, too, employs signal timing to determine position, but the mobile locator is a receiver and the orbiting satellites are transmitters. The satellites transmit spread-spectrum signals on two frequency bands denoted L1 (1575.42 MHz) and L2 (1223.6 MHz). The signals are modulated by two pseudorandom noise codes, the precision (P) code, and coarse/acquisition (C/A) code. The GPS signal is further modulated with a data message known as the GPS navigation message.

Only the C/A code in the L1 band is used in civilian applications and hence is of interest here.

To acquire the satellites' signals, the GPS receiver generates a replica of the satellites' pseudorandom noise codes. The GPS navigation message can be demodulated only if the replica can be matched and synchronized with the pseudorandom noise codes received. If the receiver cannot match and synchronize its replica, the GPS signal appears to the receiver as noise. Matching the pseudorandom noise codes and using the satellites' navigation message also enables the receiver to calculate the signal transmit time as well as the coordinates of the satellites.

The accuracy of GPS position calculations depends partly on measurement accuracy and partly on satellite configuration. Measurement errors depend on physical parameters, such as ionospheric delays and orbital uncertainties and on the selective availability factor, introduced by the U.S. Department of Defense to degrade satellite data for nonmilitary users. Total measurement errors are estimated at 35 meters; without selective availability, they are reduced to 8 meters.

The configuration of the GPS satellites at the time of the measurements adds further distortion. If those in sight are scattered throughout the sky, the measurement error is multiplied by about 1.5. If they are clustered together, the multiplier is 5 or more.

To estimate actual position accuracy, it is necessary to combine the measurement errors with the errors introduced by the spatial disposition of the satellites. To determine its position, a GPS receiver calculates its x, y, and z coordinates as well as the time the satellite signals arrive. Data must be acquired from at least four (and preferably more) observable GPS satellites. When fewer than four satellites are in view, in areas such as city canyons, one remedy is a hybrid approach, augmenting GPS with the land-based measurements called "forward link trilateration." To illustrate, the use of two GPS satellites and two cellular base stations would suffice to determine a locator's position.

The unobstructed line of sight to the orbiting transmitters is important. The satellite signals are weak (below 10^{15} W) when they arrive at a receiver's antenna and are further weakened upon entering a building. Moreover, a conventional GPS receiver could take several minutes to acquire the satellite signals and, therefore, tends to operate continuously rather than be turned on and off for each acquisition. The drain on the receiver's battery is significant.

Server-Assisted GPS

To combat the shortcomings of GPS, an innovative technique known as "server-assisted GPS" was introduced in 1998. The idea is to place stationary servers throughout the area of coverage to assist mobile receivers to acquire the GPS signals. In effect, the servers are stationary GPS receivers that enhance the mobile GPS receiver's capabilities by helping to carry their weak signals from satellites to locator. The server includes a radio interface for communicating with the mobile GPS receiver and its own stationary GPS receiver, whose antenna has full view of the sky and monitors signals continuously from all the satellites within view.

To ask a mobile GPS receiver for its position, the server feeds it satellite information through the radio interface. Included in this information is a list of observable GPS satellites and other data that enable the mobile receiver to synchronize and match its pseudo-random noise code replicas with those of the satellites. Within about a second, the GPS receiver collects sufficient information for geolocation computation and sends the data back to the server. The server can then combine this information with data from the satellites' navigation message to determine the position of the mobile device.

With the assisted GPS approach, the mobile receivers conserve power by not continuously tracking the satellites' signals. Moreover, they have only to track the pseudorandom noise code and not extract the satellites' navigation message from the signal, in effect becoming sensitive enough to acquire GPS signals inside most buildings.

In addition, the assisted version of the technology attains greater accuracy. Because the actual position of the stationary GPS receiver is known, the difference between that and its measured position can be used to calculate a correction to the mobile receiver's position. In other words, assisted GPS is inherently differential GPS (DGPS), which counters some of the inaccuracy in civilian GPS service.

The most accurate GPS service is reserved for military use.

In June of 2000, Lucent Technologies Inc., of Murray Hill, New Jersey, announced that its wireless assisted GPS had attained an accuracy of better than 5 meters outdoors—an achievement attributable to the DGPS capability of assisted GPS. More good news in this field was announced by SiRF Technology Inc., of Santa Clara, California, in the form of a postage-stamp-sized chipset (Star II) with built-in DGPS. In addition to providing improved GPS capability, it also offers reduced power consumption and greater accuracy, as well as performing well at handling weak signals.

Enhanced Signal Strength

If no obstructions are present, computing the position of a mobile locator is straightforward for both the signal timing and signal strength methods. When timing is used, the speed of light multiplied by the time a signal takes to propagate between the two points gives the distance between them.

For the signal strength method, the distance between two points can be determined from the signal attenuation between the points. However, direct line contact seldom exists inside buildings, where signal attenuation is usually unknown and many indirect paths between transmitter and receiver are likely. Although techniques exist for reducing this multipath effect, the effect cannot be eliminated, and the errors it produces are difficult to predict. Multipath effects impede signal timing methods somewhat, but affect signal strength methods even more.

In addition, signal strength is very sensitive to antenna orientation, attenuation by obstructions, and other operating conditions. In contrast, signal timing is unaffected by antenna orientation and is less sensitive to attenuation.

Nonetheless, an enhanced signal strength (ESS) method that overcomes such impediments as multipath effects, attenuation, and antenna orientation has allowed the deployment of personal locator systems in PHPS service areas in Japan. Such a system takes in three-dimensional information on the lay of the land, buildings, elevated highways, railroads, and other obstructions and uses it to simulate the RF signal propagation characteristics of every PHPS wireless transmitting antenna in the area of interest. The location system center stores the results in an RF database.

The position of a mobile locator is determined by getting it to measure the signal strength of preferably three to five base stations. From this input plus information from the base stations' databases, the system can calculate the position of the locator. The mean accuracy of the ESS is 40–50 meters. Inside large public buildings, with a PHPS base station on every floor, the system can indicate a specific floor level. In subway and railroad stations, the availability of base stations makes it possible to find an individual on a specific track.

The stand-alone locator used by Locus Corp.'s ESS method weighs only 58 grams and can operate for 16 days on a single battery charge. The ESS geolocation capabilities are also available in a standard PHPS phone handset, in which the firmware has been modified. Presently, researchers in Japan are investigating how to apply ESS technology to other wireless phone systems.

Location Fingerprinting

Instead of exploiting signal timing or signal strength, a new technique from U.S. Wireless Corp., of San Ramon, California, relies on signal structure characteristics. Called "location fingerprinting," it turns the multipath phenomenon to surprisingly good use: by combining the multipath pattern with other signal characteristics, it creates a signature unique to a given location.

U.S. Wireless's proprietary RadioCamera system includes a signal signature database of a location grid for a specific service area. To generate this database, a vehicle drives through the coverage area transmitting signals to a monitoring site. The system analyzes the incoming signals, compiles a unique signature for each square in the location grid, and stores it in the database. Neighboring grid points are spaced about 30 meters apart.

To determine the position of a mobile transmitter, the RadioCamera system matches the transmitter's signal signature to an entry in the database. Multipoint signal reception is not required, although it is highly desirable. The system can use data from only a single point to determine location. Moving traffic, including vehicles, animals, and people and changes in foliage or weather do not affect the system's capabilities.

What's PLS Good For?

In the United States, the need to provide wireless phone users with emergency 911 services has been one of the spurs to the development of location technologies. Today, an E-911 emergency call made over a land line is routed to a public safety answering point (PSAP), which matches the caller's number to an entry in an automatic location information database. When the match is made, this database provides the PSAP with the street address plus a location in a building—maybe the floor or office of the caller handset. So quickly is the caller located that the emergency crew can respond within 5 to 7 minutes on average.

The very mobility of wireless handsets rules out a simple database relationship between phone number and location. In fact, the response to a wireless call can be 10 times longer than for a land-line call—far from ideal in an emergency.

Accordingly, the U.S. Federal Communications Commission (FCC) directed operators of wireless phone services to enable their E-911 services to locate callers. The directive specified two phases. The first required an accuracy of several kilometers by April 1998 and the second required an accuracy of 125 meters with 0.67 probability by 2002. Whereas the first phase needed only software changes to the system, the second required the adoption of new location technologies.

The original FCC directive for Phase II also required support for existing handsets, which implied that only network upgrades would be acceptable. However, a network-only solution would preclude the use of emerging technologies, such as assisted GPS, because that would require handset modification in addition to any network infrastructure and software changes. All users might not bring in their handsets for modification, severely complicating support for handsets already in service.

To ease the introduction of new technologies, in September 1999, the FCC modified its original Phase II directive to permit handset-enabled solutions and also to tighten the accuracy required. In addition to the many technical roadblocks to implementing the E-911 directive, an even greater obstacle is cost. Upgrading all the wireless networks will cost billions of dollars. Cost recovery is the central issue for cellular service providers. Although wireless subscribers are the most likely source of recouping the cost, the government has made no formal decisions yet.

Presently, only the U.S. government requires its wireless companies to add caller geolocation to their E-911 services, but as the United States is a major telecommunications market, many manufacturers of wireless telecommunications equipment elsewhere are developing approaches to meet the commission's directive.

In an international development, a working group of the European Telecommunications Standards Institute (ETSI), based in Sophia Antipolis, France, is currently drafting a standard for supporting location services for the Global System for Mobile Communications (GSM). Currently, GSM is the most common mobile wireless system in the world and is available in more countries than any other wireless system.

Monitoring Tops Services List

Wireless E-911 just helps the individual, but monitoring the mentally impaired and criminals could have even greater impacts on society at large. With the changing demographics of the developed world, the percentage of individuals over age 65 will soar over the next several decades. So will the number of elderly afflicted with age-related mental impairments. Most of the eight million or so U.S. patients diagnosed with Alzheimer's disease are over age 65.

Recall how personal locator technology helped a family find a mentally impaired elderly man, fortunately within 50 minutes or so. What if many hours passed before anyone noticed that the man was missing? What if he had run into some kind of difficulty during that time? Being mentally impaired, he would be unlikely to press the panic button. An automatic polling system could solve this problem by checking whether the man was within a defined polygonal area or not—the location service and the family would be alerted whenever the man went out of this area.

As the population ages, the need for and cost of long-term care are likely to increase, too. Today it costs over $70,000 per year in the United States to care for a patient in a nursing home. Systems that monitor the whereabouts of the mentally impaired elderly could help them live longer in their communities and spend less time in institutions.

Criminal justice is another area of social concern where personal locators could intervene. The United States leads industrial nations in the percentage of its population incarcerated. In 2003, according to U.S. Department of Justice statistics, almost 8.5 million people were serving time in U.S. jails and prisons, and a further 11 million were in parole and probation programs. In comparison, in Japan in 2003, only 468,000 were serving prison terms while 423,000 were on parole or probation.

The high human and monetary cost of corrections could be reduced by new technologies, such as PLSs, that would reduce prison populations and improve the monitoring of parolees and persons on probation. First-generation monitoring systems, introduced in the mid-1980s, track the location of the offender in a very confined area, such as the home. They enable the corrections system to verify that a parolee stays there during specified periods, 6 P.M. to 6 A.M., for example, but by day, when the offender is presumably at work, these systems can do nothing.

Second-generation monitoring systems do better. A tamperproof personal locator is fastened on the offender and tracked continuously and automatically over a wide area. The newer system compares the actual with the supposed positions of the offender, as stored in a database. If any violation or tampering with the locator occurs, the system alerts the appropriate corrections or law enforcement agencies.

The goal is to verify that parolees and probationers comply with the directives imposed by the corrections system as to where and when they should and should not be by day and night. For example, a child molester is excluded from school areas, and a stalker is excluded from areas near the home and workplace of the victim.

Storage of the offender's ongoing whereabouts in an electronic file benefits law enforcement agencies in other ways [6]. The record can be used to exclude or include a monitored offender as a suspect in a crime by comparing events at the crime scene with the file entries.

Privacy, Security Still Issues

Confidentiality of information about a person's whereabouts is a serious concern for location technology. Databases already store large amounts of personal information, including medical data, marketing preferences, and credit information. Lax security could lead to serious abuse of this data. Access to a database of location information could aggravate this situation by further exposing a person's movements. Moreover, it can have real-time implications. For example, someone could find and harm a victim.

The location information stored in databases needs to be secured, as does the tracking and locating process itself. Because RF communications are used, eavesdropping is a possibility. To reduce this risk, location information can be encrypted or transmitted using coded signals employing such spread-spectrum technology as CDMA.

Privacy protection can also depend on the technology used. For example, in GPS or the ESS method, the location system uses information captured and transmitted by the locator. Some devices are equipped with an option to block such transmissions, preventing the system from locating the device. In network-based locator systems that measure the locator's signal characteristics without requiring its cooperation, the only safe way for users to keep their locations secret is to turn off the device.

More Work to Be Done

Despite the strides made in recent years in personal locator technologies, much work remains to be done on their accuracy, locator miniaturization, battery life, multipath effects, ability to penetrate buildings, and the economical use of RF bandwidth. In addition, hybrid systems may be required to provide improved coverage and open the door to new applications.

Reducing the cost of deploying location technology is essential in removing barriers to the use of location services. The concern over how to pay for E-911 services demonstrates the need for cost reduction. However, if a rich set of location services could share the expense of the additional infrastructure needed to support these services, the cost per subscriber would be reduced. The new location technologies, as well as wireless data packet services that are now emerging around the globe, offer opportunities for entrepreneurs to expand personal locator services.

In June 2002, Loc8.net (*http://www.loc8.net*), based in Seattle, Washington, began to provide location-based services employing the ReFLEX two-way paging wireless infrastructure. The services use wireless assisted GPS and include personal locator services for Alzheimer patients and children, as well as commercial services such as fleet management. The two-way paging systems using ReFLEX, developed by Motorola Inc. of Schaumberg, Illinois, cover 98% of the U.S. population. The Loc8.net system operates in emergency and paging modes.

Recent advances such as assisted GPS are likely to enhance GPS-based offender-monitoring systems, reducing device size and power consumption, adding to accuracy, and offering new capabilities such as in-building tracking. In the future, personal locators could bring many other blessings. Equipping young children with personal locators may offer parents greater peace of mind. Small enough locators could even track pets.

Personal locators could also be helpful to medical patients where the locator would be combined with a detector that monitors the patient's vital signs. If the detector picked up abnormalities in the signals, it would alert the nurse or physician with both medical and location information. Such a service could offer a patient greater freedom and a shorter stay in hospital or nursing home. Its greatest contribution, however, may be peace of mind for patients, their families, and doctors.

Obviously, technical and commercial considerations will determine the success of the technology. Issues of users' privacy and confidentiality will, however, have to be addressed first.

THE IMPLICATIONS OF COOKIES AND INTEGRATED PLATFORMS

Cookies have benefits and drawbacks. Used properly, they can enhance a visitor's experience of a Web site. Used carelessly, they can poison a user's impression of a site and even prompt some users to stay away forever.

All Web site integrated platform designers will eventually face the question of whether and how to use cookies. Often, designers find themselves ill-equipped to make this decision and so they employ cookies haphazardly or without regard for user acceptance or data privacy.

This section is for anyone involved in Web site integrated platform design, not just engineers, so it avoids addressing every low-level technical nuance of cookies. Instead, it explores technical considerations, interface design challenges, and (perhaps most importantly) ethical issues.

A Cookie in a Nutshell

When a visitor views a Web page, the server can assign that visitor a unique customer ID, known as a cookie. The server asks the visitor's browser program to "accept" the cookie—to save the ID number on the visitor's computer. Then the browser sends the cookie back to the Web server each time the visitor returns to that page, or in some cases, to any page on the Web site.

The ID number tells the server that the visitor has visited the site in the past. The server can use the ID number as a key to store any information the visitor has provided in past visits, or any details it has observed about the visitor's preferences or browsing behavior. The ID number can save a visitor from having to repeatedly log-in to a members-only site on each visit.

Why Cookies Provoke Controversy

Cookies (like any powerful data-gathering tool) can be abused. Many users fear, sometimes justifiably, that a cookie they accept may allow unscrupulous Web site operators to gather information about them and then use that data in an unauthorized manner. These users set their browser software to warn them of each incoming cookie—and many users reject every cookie, without exception.

NOTE

Web site integrated platform designers should note this sometimes justified mistrust in cookies and design accordingly.

Poor Support of Cookies in Browsers

Part of the climate of mistrust surrounding cookies stems from the poor cookie interface provided by current Web browser software. Both Netscape and Microsoft browsers can consult users before accepting a cookie, and many users choose to browse with this preference turned on.

Currently, a visitor who rejects a cookie on a Web site integrated platform but continues to browse experiences a relentless barrage of cookie requests. Often, even visitors who accept a cookie are still bombarded by offers of more cookies from the same site. On many sites, this badgering can include multiple cookies per page, cookies that change gratuitously even once accepted, and cookies on pages that don't even require cookies for any apparent reason. As feedback from users reaches the designers of browser software, look for browsers to add the following features to help users cope with this overuse of cookies:

- Reject all cookies option
- Better choices when asked
- Cookie management tools

Reject All Cookies Option

Today, browsers present only the annoying false choice between "Accept all cookies without asking" and "Ask about each cookie." Users should expect to see these choices expanded to include a third "Reject all cookies without asking" option.

Better Choices When Asked

For users who choose notification, browsers should offer a more flexible set of choices regarding what happens after a cookie has been accepted or rejected. Specifically, the user should be able to say "I want to accept/reject this cookie, and then don't ask me again..."

- About this particular cookie on this Web site integrated platform
- About any cookie on this Web site integrated platform
- About any cookie on this page

Cookie Management Tools

Finally, expect to see browsers offer a mechanism that lets users view and manage the set of cookies they've collected. Certain browsers, such as the most recent release of Microsoft Internet Explorer, have begun to add these or similar cookie management features. Until a majority of common browsers have incorporated these options, integrated platform designers should plan to minimize the number and type of cookies a visitor encounters on a site.

WINTEL INSIDE, OR HOW YOUR COMPUTER IS WATCHING YOU

Privacy Foundation has discovered that it is possible to add "Web bugs" to Microsoft Word documents. A Web bug could allow an author to track where a document is being read and how often. In addition, the author can watch how a bugged document is passed from one person to another or from one organization to another. Some possible uses of Web bugs in Word documents include

- Detecting and tracking leaks of confidential documents from a company
- Tracking possible copyright infringement of newsletters and reports

- Monitoring the distribution of a press release
- Tracking the quoting of text when it is copied from one Word document to a new document

Web bugs are made possible by the ability in Microsoft Word of a document to link to an image file that is located on a remote Web server. Because only the URL of the Web bug is stored in a document and not the actual image, Microsoft Word must fetch the image from a Web server each and every time the document is opened. This image-linking feature puts a remote server in the position to monitor when and where a document file is being opened. The server knows the IP address and host name of the computer that is opening the document. A host name will typically include a company name if a computer is located at a business. The host name of a home computer usually has the name of a user's Internet service provider (ISP).

An additional issue, and one that could magnify the potential surveillance, is that Web bugs in Word documents can also read and write browser cookies belonging to Internet Explorer. Cookies could allow an author to match up the computer viewer of a Word document to their visits to the author's Web site.

Web bugs are used extensively for tracking by Internet advertising companies on Web pages and in HTML-based email messages. They are typically 1-by-1 pixel in size to make them invisible on the screen to disguise the fact that they are used for tracking.

Although the Privacy Foundation has found no evidence that Web bugs are being used in Word documents today, there is little to prevent their use. Short of removing the feature that allows linking to Web images in Microsoft Word, there does not appear to be a good preventative solution. However, the Privacy Foundation has recommended to Microsoft that cookies be disabled in Microsoft Word through a software patch. In addition to Word documents, Web bugs can also be used in Excel and PowerPoint documents.

Detailed Description

Microsoft Word has, from the beginning, supported the ability to include picture files in Word documents. Originally, the picture files would reside on the local hard drive and then be copied into a document as part of the Word.doc file. However, beginning with Word 97, Microsoft provided the ability to copy images from the Internet. All that is required to use this feature is to know the URL (Web address) of the image. Besides copying the Web image into the document, Word also allows the Web image to be linked to the document via its URL. Linking to the image results in smaller Word document files because only a URL needs to be stored in the file instead of the entire image. When a document contains a linked

Web image, Word will automatically fetch the image each time the document is opened. This is necessary to display the image on the screen or to print it out as part of the document.

Because a linked Web image must be fetched from a remote Web server, the server is in a position to track when a Word document is opened and possibly by whom. Furthermore, it is possible to include an image in a Word document solely for the purpose of tracking. Such an image is called a Web bug. Web bugs today are already used extensively by Internet marketing companies on Web pages and embedded in HTML email messages.

When a Web bug is embedded in a Word document, the following information is sent to the remote Web server when the document containing the bug is opened:

- The full URL of the Web bug image
- The IP address and the host name of the computer requesting the Web bug
- A Web browser cookie (optional)

This information is typically saved in an ordinary log file by Web server software.

Because the author of the document has control of the URL of the document, they can put whatever information they choose in this URL. For example, a URL might contain a unique document ID number or the name of the person to whom the document was originally sent.

These tracking abilities might be used in any number of ways. In most cases, the reader of a particular document will not know that the document is bugged or that the Web bug is surreptitiously sending identifying information back through the Internet.

One example of this tracking ability is to monitor the path of a confidential document, either within or beyond a company's computer network. The confidential document could be bugged to "phone home" each time it is opened. If the company's Web server ever received a "server hit" from an IP address for the bug outside the organization, then it could learn immediately about the leak. Because the server log would include the host name of the computer where the document was opened, a company could know that the organization that received the leaked document was a competitor or media outlet, for example.

All original copies of a confidential document could also be numbered so that a company could track the source of a leak. A unique serial number could be encoded in the query string of the Web bug URL. If the document is leaked, the server hit for the Web bug will indicate which copy was leaked.

A serial number could be added to a Web bug in a document either manually (right before a copy of a document is saved) or automatically through a simple utility program. The utility program would scan a document for the Web bug URL and add a serial number in the query string. A Perl script of less than 20 lines of code could easily be written to do this sort of serialization.

Another use of Web bugs in Word documents is to detect copyright infringement. For example, a publishing company could bug all outgoing copies of its newsletter. The Web bugs in a newsletter could contain unique customer ID numbers to detect how widely an individual newsletter is copied and distributed.

A third possible use of Web bugs is for market research purposes. For example, a company could place Web bugs in a press release distributed as a Word document. The server log hits for the Web bugs would then tell the company what organizations have actually viewed the press release. The company could also observe how a press release is passed along within an organization or to other organizations.

In an academic setting, Web bugs might be used to detect plagiarism. A document could be bugged before it is distributed. An invisible Web bug could be placed within each paragraph in the document. If text were to be cut and pasted from the document, it is likely that a Web bug would be picked up also and copied into the new document

To place a Web bug in a Word document is relatively simple. These are the steps in Word:

1. Select the Insert | Picture | From File menu command.
2. Type in the URL of the Web bug in the File Name field of the Insert Picture dialog box.
3. Select the Link to File option of the Insert button.

The use of Web bugs in Word does point to a more general problem. Any file format that supports automatic linking to Web pages or images could lead to the same problem. Software engineers should take this privacy issue into consideration when designing new file formats.

This issue is potentially critical for music file formats such as MP3 files where piracy concerns are high. For example, it is easy to imagine an extended MP3 file format that supports embedded HTML for showing song credits, cover artwork, lyrics, and so on. The embedded HTML with embedded Web bugs could also be used to track how many times a song is played and by which computer, identified by its IP address.

DATA MINING FOR WHAT?

The use of data mining for IW is growing rapidly. The number of data-mining consultants, as well as the number of commercial tools available to the “nonexpert” user, are also quickly increasing. It is becoming easier than ever to collect datasets and apply data-mining tools to them. As more and more nonexperts seek to exploit this technology to help with their business, it becomes increasingly important that they understand the underlying assumptions and biases of these tools. There are a number of factors to consider before applying IW data mining to a database. In particular, there are important issues regarding the data that should be examined before proceeding with the data-mining process. Although these issues may be well-known to the data-mining expert, the nonexpert is often unaware of their importance.

Now let's focus on three specific issues. Each issue is illustrated through the use of brief examples. Also, insight is provided for each issue on how it might be problematic, and suggestions are made on which techniques can be used for approaching such situations.

The purpose here is to help the nonexpert in IW data mining better understand some of the important issues of the field. Particular concern is also established here with characteristics of the data that may affect the overall usefulness of the IW data-mining results. Some recent experiences, and the lessons learned from them, are described. These lessons, together with the accompanying discussion, will help to both guide the IW data-collection process and better understand what kinds of results to expect.

One cannot blindly "plug-and-play" in IW data mining. There are a number of factors to consider before applying data mining to any particular database. This general warning is not new. Many of these issues are well known by both the data mining experts and a growing body of nonexpert, data owners. For instance, the data should be "clean," with consistent values across records and containing as few errors as possible. There should not be a large number of missing or incomplete records or fields. It should be possible to represent the data in the appropriate syntax for the required data-mining tool (attribute/value pairs).

This section will discuss three specific, but less well-known, issues. Each will be illustrated through real-world experiences. The first is the impact of *data distribution*. Many IW data-mining techniques perform class or group discrimination and rely on the data-containing representative samples of all relevant classes. Sometimes, however, obtaining samples of all classes is surprisingly difficult. The second issue is one of *applicability and data relevance*. High-quality data, combined with good data-mining tools, does not ensure that the results can be applied to the desired goal. Finally, this section will discuss some of the issues associated with using *text* (narrative fields in reports) in data mining. The current technology cannot fully exploit arbitrary text, but there are certain ways text can be used.

These three issues are not new to the field. Indeed, for many IW data-mining experts, these are important issues that are often well understood. For the nonexpert, however, these issues can be subtle or appear deceivingly simple or unimportant. It is tempting to collect a large amount of clean data, massage the representation into the proper format, hand the data tape to the consultant, and expect answers to the most pressing business questions. Although this section does not describe all of the potential problems one might face, it does describe some important issues, illustrate why they might be problematic, and suggest ways to effectively deal with these situations.

Two Examples

The discussion of data distribution, information relevance, and use of text will be illustrated with examples from two current projects. The first involves a joint project with the Center for Advanced Aviation Systems Development (CAASD) in the domain of aviation safety. In this project, one of the primary goals is to help identify and characterize precursors to potentially dangerous situations in the aviation world. One particular way to do this is to mine accident and incident reports involving aircraft for patterns that identify common precursors to dangerous situations. For any type of flight—commercial, cargo, military, or pleasure—accidents (and often less serious incidents) are investigated. A report is filed containing a variety of information such as time of day, type of aircraft, weather, pilot age, and pilot experience. These reports often include the inspector's written summary. One task involves using collections of these reports to try to identify and characterize those situations in which accidents occur. A source of such reports is the National Transportation Safety Board (NTSB).

Another project we are currently working on involves targeting vehicles for law enforcement. In this particular instance, vehicles (mostly passenger vehicles and small trucks) arrive at an inspection stop. At this primary stop, a brief inspection is conducted to decide if further examination is necessary. There is typically a constant flow of cars to be processed, so excessive time cannot be taken. This first inspection typically takes 20 to 30 seconds. If the primary inspector feels it is warranted (and there are any number of reasons that justify this), any vehicle can be pulled out for secondary inspection. This secondary inspection and background check is more thorough. If the driver or vehicle is found to be in violation of the particular laws under consideration, then information concerning both driver and vehicle is collected and entered into the "violators" database. The goal of this project is to find a way to better profile these violating drivers and vehicles, so that the primary inspectors can more accurately identify likely suspects and send them for secondary inspection.

Data Distribution

Let's first discuss the issue of data distribution. Of particular concern is the situation in which the data lacks certain types of examples. Consider the aviation safety domain. One goal of the project in this domain is to characterize situations that result in accident flights. An obvious source of information is the NTSB's database of accident reports.

NOTE

This database does not contain records about uneventful flights (the NTSB is an accident investigation agency). That is, the data are unevenly distributed between records of accident flights and records of uneventful flights.

This lack of reports about uneventful flights has important consequences for a significant class of data-mining techniques. When given the data containing only accident flights, each of the approaches in this class concludes that all flights contain accidents. Such a hypothesis is clearly incorrect. The majority of the flights are uneventful. Also, such a hypothesis is not useful because it does not offer any new insight on how to differentiate the accident flights from the uneventful ones. Furthermore, some of the most popular IW data-mining tools, including decision tree inducers, neural networks, and nearest neighbor algorithms, fall into this class of techniques. (They assume that the absence of uneventful flights in the data implies that they do not exist in the world.)

To continue this discussion, it is necessary to first define some terms used in data mining. The "target concept" is the concept you are trying to learn. In the aviation domain, the target concept is accident flights. Consequently, each example of an accident flight (each accident report in the database) is called a member of the target concept, and each uneventful flight is a nonmember of the target concept. The NTSB data do not contain records of uneventful flights. That is, there are no descriptions of nonmembers of the target concept. The problem of learning to differentiate members from nonmembers is called a "supervised concept learning problem."

NOTE

It is called supervised because each example in the data contains a label indicating its membership status for the target concept.

For example, a supervised concept learner uses a training sample as input. A training sample is a list of examples, labeled as members or nonmembers, which is assumed to be representative of the whole universe. The supervised concept learner produces hypotheses that discriminate the members and nonmembers in the sample. Many IW data-mining tools use supervised concept learners to find patterns.

Let's say that a supervised concept learner makes the closed-world assumption that the absence of nonmembers in the data implies that they do not exist in the universe. Why do some of the popular learners make the closed-world assumption? The case of decision tree learners provides a good illustration. These learners partition the training sample into pure subsamples, containing either all member or all nonmembers. The partitioning of the training sample drives the rule generation. That is, the learners introduce conditions that define partitions of the training sample; each outcome of a condition represents a different subsample. Ultimately, the conditions will become part of the discrimination rules. Unfortunately, if the input sample contains only data that are members of the target class, the training sample is already pure and the decision tree learner has no need to break up the sample further. As a consequence, the rules commit to classifying all new data as members of the target class before conducting any tests. Thus, in the aviation project, all flights would be classified as accident flights, because the learner never saw any uneventful flights. This is not to say that learners employing the closed-world assumption are inappropriate in all, or even most situations. For many problems, when representative data from all the concepts involved is available, these learners are both effective and efficient.

Applicability and Relevance of Data

Even when collected data is of high quality (clean, few missing values, proper form, etc.) and the IW data-mining algorithms can be successfully run, there still may be a problem of relevance. It must be possible to apply the new information to the situation at hand. For instance, if the data mining produces typical "if...then..." rules, then it must be possible to measure the values of the attributes in the condition ("if" part) of those rules. The information about those conditions must be available at the time the rules will be used. Consider a simple example where the goal is to predict if a dog is likely to bite. Assume data are collected on the internal anatomy of various dogs, and each dog is labeled by its owner as either "likely" or "unlikely" to bite. Assume further that the data-mining tools work splendidly, and it is discovered that the following (admittedly contrived) rules apply: Rule 1: If the rear molars of the dog are worn, the dog is unlikely to bite. Rule 2: If the mandibular muscles are over-developed, the dog is likely to bite.

These may seem like excellent rules. However, if faced with a strange, angry dog late at night, these rules would be of little help in deciding whether you are in danger. There are two reasons for this: First, there is a time constraint in applying the rules. There are only a few seconds to check if these rules apply. Second, even without such a constraint, the average person probably can't make judgments about molar wear and muscle development. The lesson here is that just because data are collected about biting (and nonbiting) dogs, it does not mean one can predict whether a dog will bite in every situation.

In the vehicle-targeting task described earlier, a similar situation occurred. The initial goal was very specific: develop a set of rules, a profile, that the primary inspectors could use to determine which vehicles to pull out for secondary inspection. As mentioned, much more information is collected concerning actual violators than for those who are just passed through the checkpoint. Thus, the initial goal was to profile likely violation suspects based on the wealth of information about that group. The problem, noticed before any analysis was done, was that the information that would make up the profiles would not be applicable to the desired task.

As mentioned, the primary inspectors have only a short amount of time to decide whether a particular vehicle should be pulled out for secondary inspection. During that time, they have access to only superficial information. That is, the primary inspectors don't have quick access to much of the background knowledge concerning the driver and vehicle, yet this is precisely the knowledge collected during seizures initially chosen to build profiles. Thus, they have no way to apply classification rules that measure features such as "number of other cars owned," "bad credit history," or "known to associate with felons" (types of data collected on violation vehicles and drivers).

The problem here is not that the data is "bad," or even that the data is all from the target concept. The problem is that the data cannot be applied to the initially specified task. How does this situation come about in general? The answer involves a fairly common situation. Often, IW data mining begins with data that has been previously collected, usually for some other purpose. The assumption is made that since the collected data is in the same general domain as the current problem, it must be usable to solve this problem. As the examples show, this is often not the case. In the vehicle-targeting task, the nature of the law enforcement system is such that a great deal of information is collected and recorded on violators. No one ever intended to use this information as a screening tool at stop points. Thus, it is important to understand the purpose for which a set of data was collected. Does it address the current situation directly? Similarly, when data is collected for the specific task at hand, careful thought must go into collecting the relevant data.

There are two primary ways to address this problem of data irrelevancy. The most obvious is to use additional data from another source. It may be that different data already exists to address the primary question. For instance, returning to the example of the dogs, general aggressiveness characteristics for different breeds of dogs have been determined. Using this data, rather than the original data, deciding how likely a dog is to bite is reduced to the problem of determining its breed (often done by quick visual inspection). When the necessary data does not already exist, it may be necessary to collect it. Some of this data collection will likely take place in the vehicle-targeting project. In this case, data must be collected that relates directly to the information available to the inspectors at the initial inspection. For example, the demeanor of the driver may be an important feature. Of course, collecting new data may be a very expensive process. First, the proper attributes to collect must be determined. This often involves discussions and interviews with experts in the field. Then the actual data-collection process may be quite costly. It may be that an inordinate amount of manpower is required, or that certain features are difficult to measure.

If additional data cannot be obtained, there is another, often less desirable way to address this issue. It may be possible to alter the initial goals or questions. This will clearly require problem-specific domain expertise to address a few simple questions:

Is there another way to address the same issue? Is there another relevant issue that can be addressed directly with this data? In the vehicle-targeting domain, only those attributes that were directly accessible to the inspector were used. A good example would be looking at simple statistical patterns for time of day, weather, season, and holidays. This is not a deep analysis and doesn't quite "profile" likely violators, but it makes progress toward the initial goal. Another alternative is to use the violator database to profile suspects for other situations. It may be that profiles of certain types of violators bear similarities to other criminal types. Perhaps this information can be used elsewhere in law enforcement. Admittedly, this latter solution does not address the initial issue: helping the primary inspectors decide who to pull out for secondary inspection. However, it may not be possible to achieve that goal with this data and the given time constraints. It is important to understand this potential limitation early in the process, before a great deal of time, effort, and money has been invested.

Combining Text and Structured Data

IW data mining is most often performed on data that is highly structured. Highly structured data has a finite, well-defined set of possible values, as is most often seen in databases. An example of structured data is a database containing records describing aircraft accidents that includes fields such as the make of an airplane and the number of hours flown by the pilot. Another source of valuable yet often unused information is unstructured text. Although more difficult to immediately use than structured data, data mining should make use of these available text resources.

Text is often not used during IW data mining because it requires a preprocessing step before it can be used by available tools such as decision trees, association rule methods, or clustering. These techniques require structured fields with clearly defined sets of possible values that can be quickly counted and matched. Such techniques sometimes also assume that values are ordered and have well-defined distances between values. Text is not so well behaved. Words may have multiple meanings depending on context (polysemy); multiple words may mean the same thing (synonymy) or may be closely related (hypernymy). These are difficult issues that are not yet totally solved, but useful progress has been made and techniques have been developed so that text can be considered a resource for data mining.

One way to exploit text, borrowed from information retrieval, is to use a vector-space approach. Information retrieval is concerned with methods for efficiently retrieving documents relevant to a given request or query. The standard method for doing this is to build weight vectors describing each document and then compare the document vector to the query vector. More specifically, this method first identifies all the unique words in the document collection. Then this list of words is used to build vectors of words and associated weights for the query and each of the documents. Using the simplest weighting method, this vector has a value of 1 at position x when the xth vocabulary word is present in the document; otherwise it has a value of 0. Every document and query is now described by a vector of length equal to the size of the vocabulary. Now each document vector can be compared to every other document by comparing their word vectors. A cosine-similarity measure (which projects one vector along another in each dimension) will then provide a measure of similarity between the two corresponding documents. Surprisingly, although this approach discards the structure in the text and ignores the problems of polysemy and synonymy altogether, it has been found to be a simple, fast baseline for identifying relevant documents.

A variant of this vector-space approach was used on the airline safety data to identify similar accidents based on a textual description of the flight history. The narrative description of each accident was represented as a vector and compared to all other narratives using the approach described earlier. One group of accidents identified by this technique can be described as planes that were "veering to the left during takeoff." The following accident reports were found to be similar in this respect:

> MIA01LA055: During takeoff roll he or she applied normal right rudder to compensate for engine torque. The airplane did not respond to the pilot input and drifted to the left.
>
> ANC00LA099: Veered to the left during the first attempt to take off.
>
> ANC00LA041: Pilot added full power and the airplane veered to the left.

Identifying this kind of a group would be difficult using fixed fields alone. This technique can also be used to find all previous reports similar to a given accident or to find records with a certain combination of words. This can be a useful tool for identifying patterns in the flight history of the accident so that the events leading up to different accidents can be more clearly identified.

The information stored in text can be extracted in other ways as well. A collection of documents and a taxonomy of terms are combined so that maximal word or category associations can be calculated. It could also be used in the airline safety domain to calculate, for example, which class of mechanical malfunctions occurred most often in winter weather.

Another approach relevant to IW data mining from text is information extraction (IE). IE concerns techniques for extracting specific pieces of information from text and is the focus of the DARPA Message Understanding Conference (MUC). The biggest problem with IE systems is that they are time-consuming to build and domain specific. To address this problem a number of tools have (and continue to be) developed for learning templates from examples such as CRYSTAL, RAPIER, and AutoSlog. IE tools could be used in the airline safety data to pull out information that is often more complete in the text than in the fixed fields. This work is geared toward filling templates from text alone, but often the text and structured fields overlap in content.

An example of just such an overlap can be found in the NTSB accident and incident records. The data in the NTSB accident and incident records contains structured fields that together allow the investigator to identify human factors that may be important to the accident scene. However, it was found that these fields are rarely filled out completely enough to make a classification: 95% of the records that were identified as involving people could only be classified as "unknown." IE methods could be used to reduce this large unknown rate by pulling information out of the narrative, which described if a person in the cockpit made a mistake. Such an approach could make use of a dictionary of synonyms for "mistake" and a parser for confirming if the mistake was an action made by the pilot or copilot and not in a sentence describing, for example, the maintenance methods.

Although IW data mining has primarily been concerned with structured data, text is a valuable source of information that should not be ignored. Although automatic systems that completely understand the text are a still a long way off, one of the surprising recent results is that simple techniques, which sometimes completely ignore or only partially address the problems of polysemy, synonymy, and complex structure of text, still provide a useful first cut for mining information from text. Useful techniques, such as the vector-space approach and learned templates from information extraction, can allow IW data miners to make use of the increasing amount of text available online.

THE INTERNET IS BIG BROTHER

How prepared is your business for the future? As the Internet expands its reach to the farthest corners of the globe, companies will find themselves dealing with increasingly complex challenges such as Big Brother.

In the Internet of tomorrow you can be sure of at least three things. First, the experience will not be anything like what we're familiar with. Second, despite this, little will change in the next 10 years. Third, the business environment of the future will be much less forgiving, so companies that do not take the new technologies seriously are putting themselves at risk.

Fiber Optics

During the 1990s, everyone heard about fiber-optic technology's potential for increasing bandwidth and enhancing performance. Recently, better installation techniques and a wider range of fiber-compatible equipment have made fiber both easily available and less expensive than it used to be.

Although fiber will remain a good choice for backbones and carrier-class interconnections, most companies will probably continue to run copper, at least for the foreseeable future. After all, few businesses want to bear even slightly higher costs for fiber installation and networking gear. Instead, expect to see more companies upgrading their existing copper technology. Expect them to get away with it, too, because for most practical purposes, copper can handle the load.

Broadband

High-speed Internet connections, especially the cable modem [7] and DSL technologies lumped together under the "broadband" heading, are increasing in number at an astonishing rate, at least in first world countries like the United States and within the European Union. The biggest problem the providers face seems to be keeping up with demand. The current waiting list of DSL and cable access orders probably won't be caught up until 2006. Even then, North America will be home to wide swaths of rural territory without high-speed access.

This scenario isn't likely to change in the next decade, either. Unless governments (Big Brother) insist that Internet carriers supply rural service at a loss (as American telephone companies were ordered to do with voice service), broadband providers will have little incentive to deploy their technologies on a wide scale.

The increasing availability of broadband wireless connections is another revolution that's already under way, although it won't make a serious difference anytime soon either. In its infant state, broadband wireless, with its ability to support certain e-business applications, is best suited to a LAN-like role. It will be a while before we see a device that combines the size of the cell phone with the power of the laptop.

A Truly Global Internet

The days of Americans (Big Brother) ruling the Internet are not over by a long shot. Even so, the next decade will bring an explosion of Internet usage in places such as Asia and Africa. As the Internet becomes more pervasive, businesses will face an even greater shortage of skilled employees. American businesses that have traditionally relied on a foreign labor market may be caught short when those workers can find jobs at home.

As always, the spoils will go to those businesses that think ahead. We are going to see big changes, so start preparing yourself for a world ruled by broadband, culturally neutral, easily maintained wireless access. That means considering technical issues and different standards of civil rights, conduct, and privacy. The companies that do will have a head start on the competition for the next decade and maybe the next century.

THE WIRELESS INTERNET: FRIEND OR FOE?

The wireless networking engineer was working her way through the IW test range when she stopped and looked at her computer screen. Another unsecured access point, she noted. She was testing the roaming capabilities of 802.11b network devices, but as she moved their portable computers through the areas covered by the devices, other access points popped up.

This isn't surprising, because one of the nice things about wireless Internet is the ability to install the products quickly and easily, with a minimum amount of configuration. Clearly, some people around her test site (which is being kept nameless to protect the guilty) took advantage of the ease of installation but never got around to protecting their internetworks.

If Internetwork managers don't pay attention to the fact that the default condition of wireless access points is to let anyone into the network, then they may be doing just that. Those people who constitute "anyone" can include people across the street, your competitors parked outside, and malcontents who want to use your network to shield their activities. It's like installing a network port on the lamppost outside your building and asking anyone who walks by to plug in.

Fortunately, if you plan accordingly, securing your wireless Internet isn't very difficult. It just requires network administrators to take a few simple steps. First, turn off the broadcasting of your access point's extended service set identification, which lets anyone with a wireless Internet card know the address of your wireless Internet access point. Having that ID makes logging-in even easier than it already is. Second, turn on encryption. All 802.11b access points support the wireless encryption protocol (WEP), which can handle 40- and 128-bit encryption. Third, turn on your ability to use access control lists, available in some access points. This allows you to keep a list of acceptable users according to the medium access control (MAC) address of their network card.

These steps will keep most wireless networks reasonably secure. It's convenient that these capabilities are built into most wireless Internet access points—the only exception being some early Apple AirPorts, which can be upgraded.

You must also deal with the fact that wireless access points are inexpensive and that getting them running is a no-brainer. This means that pretty much anyone on your network can pick up a wireless access point at Best Buy, plug it into the corporate network, and use it. You'd then have an entry point into your network that's open to anyone with a wireless Internet card. Fortunately, if you already have a wireless Internet, you probably also have the management software that lets you locate all access points, including those that aren't authorized, and you can either take them off the network or secure them.

Another problem is that, without limits on what users are allowed to do and where they're allowed to go, you lose control. So even more security is needed. One solution is to move to a third-party provider of wireless security products, such as WRQ, whose NetMotion product requires a login that's authenticated through Windows NT. It uses much better encryption than is available under wired equivalent privacy (WEP) and it offers some security management features, such as the ability to remotely disable a wireless Internet card's connection to the network. Such capabilities require a bit more attention from managers, but the result can be a wireless Internet that's more secure than the wired one it's attached to.

Stories abound of employees who bought their own wireless access points, installed them, and claimed they were "just testing" when they were discovered. Meanwhile, these employees opened their companies' networks to anyone (friend, foe, hacker, or spy) who cared to enter.

How do you find these people who would expose your network? Oddly enough, the easiest way is for your company to start using wireless Internetworking—in an organized fashion. That eliminates the need for employees to buy their own access points, and it gives the IT department the tools it needs to detect and eliminate them.

SUMMARY

Attacks on information technology are unsettling and easy to carry out. The means are relatively inexpensive, easy to smuggle, virtually untraceable, and completely deniable. This, coupled with the fact that the civilian networks, which are most attractive to terrorists, are also the most vulnerable, makes infowar the perfect weapon in the terrorist arsenal of the future.

Currently, the security solutions lag far behind the potential threat. This situation is likely to continue until the threat becomes reality, forcing a reassessment of preventive measures. The basic concepts and principles that must be understood and can help realistically guide the process of moving forward in dealing with the surveillance tools for the IW of the future are as follows.

Conclusions

- Fortunately, the U.S. military senior leadership is becoming involved in IW, and, in many cases, taking the lead on this perplexing issue. With this emphasis, they must carefully assess the vulnerabilities of the systems they employ.
- Systems proposals must be thoroughly evaluated and prioritized by highest value payoff. This needs to be accomplished through a more balanced investment strategy by the U.S. military that conquers our institutional prejudices that favor killer systems weapons.

- Offensive systems will be at risk if the U.S. military does not apply sufficient defensive considerations in this process.
- The electromagnetic spectrum will be their Achilles' heel if the U.S. military does not pay sufficient attention to protecting their use of the spectrum and, at the same time, recognize that they must take away the enemy's ability to see the U.S. forces and to control their own forces.
- Interdict opportunities exist for adversaries to intrude on U.S. military systems.
- Other nations have realized the value of offensive applications of the IW arsenal of the future; therefore, the U.S. military must attack the issue from two directions, offensively and defensively, with almost equal accentuation.
- The IW arsenal of the future adds a fourth dimension of warfare to those of air, land, and sea. When the Soviets developed a nuclear program after World War II, the United States was caught by surprise. In this new dimension, the U.S. military must stay ahead.
- As with so many other design issues, taking the user's experience into account suggests how to proceed with implementing cookies.
- If the data contains examples of only a single class, extra work may be involved, as some popular types of data-mining methods may not be appropriate.
- Although automated understanding of natural language is not available, an increasing number of techniques can be used for exploiting text data.
- An important feature of bandwidth/packet management technology is its stealthy wireless internet security features that render complete invisibility and protection for end users from network hackers and other wireless users sharing the same access points.

An Agenda for Action

It must be pointed out that although such IW preparation measures can provide a minimum level of protection against tampering, there is no such thing as 100% security. What is more, the solutions are sure to lag behind the potential threat until the threat becomes reality. At present the cost of protection is higher than the cost of attack, and until an attack on a major system actually happens, organizations are unlikely to take security measures as seriously as they could or should. The U.S. government needs to set an agenda for action that goes beyond the work already done in preparation for defending against the surveillance tools for IW of the future. Action steps should include, but not be limited to the 11 areas shown in Table F18.1 in Appendix F.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Fortunately, the U.S. military senior leadership is becoming involved in IW and, in many cases, taking the lead on this perplexing issue. With this emphasis, they must carefully assess the vulnerabilities of the systems they employ.
2. True or False? Interdict opportunities exist for adversaries to intrude on U.S. military systems.
3. True or False? Offensive systems will be at risk if the U.S. military does not apply sufficient defensive considerations in this process.
4. True or False? The IW arsenal of the future adds a fourth dimension of warfare to those of air, land, and sea. When the Soviets developed a nuclear program after World War II, the United States was caught by surprise. In this new dimension, the U.S. military must stay ahead.
5. True or False? An important feature of bandwidth/packet management technology is its stealthy wireless Internet security features that render complete invisibility and protection for end users from network hackers and other wireless users sharing the same access points.

Multiple Choice

1. As feedback from users reaches the designers of browser software, look for browsers to add the following features to help users cope with this overuse of cookies, except:

   A. Reject all cookies option
   B. Better choices when asked
   C. Accept all cookies option
   D. Cookie management tools

2. Specifically, the user should be able to say "I want to accept/reject this cookie, and then don't ask me again...," except:

   A. About this particular cookie on this Web site integrated platform
   B. About all cookies
   C. About any cookie on this Web site integrated platform
   D. About any cookie on this page

3. Some possible uses of Web bugs in Word documents include the following, except:
   - A. Managing documents
   - B. Detecting and tracking leaks of confidential documents from a company
   - C. Tracking possible copyright infringement of newsletters and reports
   - D. Monitoring the distribution of a press release
   - E. Tracking the quoting of text when it is copied from one Word document to a new document

4. When a Web bug is embedded in a Word document, the following information is sent to the remote Web server when the document containing the bug is opened, except:
   - A. The full URL of the Web bug image
   - B. The IP address and the host name of the computer requesting the Web bug
   - C. A Web browser cookie (optional)
   - D. The near future

5. To place a Web bug in a Word document is relatively simple. These are the steps in Word, except one:
   - A. Select the Delete | Picture | From File... menu command.
   - B. Select the Insert | Picture | From File... menu command.
   - C. Type in the URL of the Web bug in the File Name field of the Insert Picture dialog box.
   - D. Select the Link to File option of the Insert button.

Exercise

The CTO of a large beverage company suspected something was amiss when he noticed a significant amount of traffic traveling through the company network. He deduced that his trusted staff of system administrators might have been misusing their access privileges and the network servers for some unknown purpose. A computer forensics specialist team (CFST) was contracted to perform a confidential after-hours investigation of the network and the system administrators. How was the CFST able to go about conducting their investigation?

HANDS-ON PROJECTS

A large multinational corporation was accused of questionable financial reporting by the SEC, resulting in an investigation by a major independent consulting company. The goal of the investigation was to determine if the Chief Financial Officer had ordered his staff to alter or destroy transactions to help the company's financial position appear more favorable. How did the CFS go about conducting the investigation?

Case Project

A CFST conducted the analysis of multiple seized computer systems taken in connection with major cases of central excise duty evasion in the Indian government. How did the CFST go about conducting the investigation?

Optional Team Case Project

The Austin Police Department (APD) covers an area of 270 square miles and over 650,000 residents of greater Austin, Texas. Austin is the state capitol, and the government offices employ approximately 20% of the population. The APD knew they had a Windows 2000/20003 file server and at least 12 workstations that needed to be analyzed from a particular business under investigation. The APD also had a system administrator who was located out of state, and they weren't sure he was trustworthy. If the APD had pulled the server from this particular business, by shutting them down, the business could have sued the city and possibly won for the loss of productivity. How did the CFS go about conducting the investigation?

REFERENCES

[1] Vacca, John R., *Wireless Data Demystified*, McGraw-Hill, New York, 2003.

[2] Vacca, John R., *Satellite Encryption*, Academic Press, New York, 1999.

[3] Vacca, John R., *Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan*, McGraw-Hill, New York, 2001.

[4] Vacca, John R., *Wireless Broadband Networks Handbook*, New York, McGraw-Hill, 2001.

[5] Vacca, John R., *i-mode Crash Course*, McGraw-Hill, New York, 2002.

[6] Vacca, John R., *The Essential Guide to Storage Area Networks*, New York, Prentice Hall, 2002.

[7] Vacca, John R., *The Cabling Handbook*, 2nd ed., Prentice Hall, New York, 2001.

19 Civilian Casualties: The Victims and Refugees of Information Warfare

National information infrastructures are becoming an important vehicle for the generation of national wealth throughout the developed world. National information systems are, among other things, already used to conduct commerce and regulate and control national production. Nations are becoming increasingly dependent on their information infrastructure as the Information Age evolves. Accordingly, this infrastructure may now be considered to represent an extension of national sovereignty, and any attacks on national information systems may be perceived as attacks on the nation itself. This has resulted in civilian causalities (the victims and refugees of information warfare [IW]).

A further argument may be that the national security implications of information attacks make the defense against such attacks a military task. If this is the case, the vast majority of the world's military forces require a significant review of their current doctrine and capabilities. Most are presently not capable of operating in a hostile information environment. An alternative argument may be that attacks against national information systems are criminal in nature and are, therefore, the responsibility of national police forces. Again, most police forces are incapable of defending against such attacks. Indeed, there is probably no organization in the world that can adequately defend national information infrastructures as of yet. Regardless of the capabilities of the various organizations, the jurisdiction boundaries that separate civilian and military security responsibilities are blurring as the Information Age evolves.

Separating military and civilian information operations, particularly as they pertain to defending national information systems, is also complicated by military dependence on the civilian information infrastructure. Significant elements of many of the information systems used by the world's modern military forces are designed, developed, and managed by civilians, primarily for civilian purposes, and make extensive use of the civilian information infrastructure. This is particularly the case with communication systems. The use of unique systems by military forces for all of their information tasks is not economically viable. Therefore, an attack that targets a military capability via a multiuser information system may inadvertently disrupt civilian users. Likewise, an attack that is directed at a civilian user of an information system may inadvertently affect military users. Is a military or civilian response more appropriate in each of these cases? To many this may appear to be a trivial issue, but distinguishing between civilian and military information operations is important if an appropriate (and legal) national response is to be determined.

Identifying the source of an information attack can be difficult, at times impossible, and can contribute to the problem of determining an appropriate response. Following a skilled information attack, identifying whether the act was calculated and hostile or simply an accident or a system error may well be impossible. Determining whether a nation, an individual, or a non-nation-state organization committed the IW attack may also be impossible, as may be ascertaining the extent of any damage caused to civilians or refugees. Given the embryonic state of international law pertaining to the information domain, pursuing a response through the courts may also be impossible or pointless. Therefore, although distinguishing between a military information operation (MIO) and a civilian information operation (CIO) is highly desirable, and, from a legal viewpoint may be essential, such distinction is often impossible.

Attempting to resolve tomorrow's information security challenges with today's security infrastructure and culture is unlikely to prove successful. Securing a national information infrastructure presents unique challenges to national security agencies and demands unique and innovative solutions.

The need for macro-level information security in the information domain is becoming more obvious. There is a strong argument for the development of a national information authority responsible for assuring the integrity of all national information systems, advising on the development of new information systems, sponsoring research and development into information-assurance technologies, and ultimately prosecuting information operations in support of diplomatic, counter-criminal, and conflict-resolution objectives.

A national information authority would offer many strategic opportunities and benefits (including significant efficiencies) and could comfortably address information issues across portfolios, including national security and defense considerations. Such an organization would not deny the individual elements of a nation's armed forces the right to develop their own information strategies; indeed, all the armed services have both a single-service and joint responsibility to develop robust information strategies now. The further a nation travels down the Information Age path, however, the more necessary the development of a professional, specialist national information body appears. It is an option that should be considered by any government with a genuine commitment to national security and the protection of its civilians.

WHAT THE CYBER MASSES HAVE TO LOSE

As explained in the preceding chapters, IW is the latest development in a long list of revolutions in military affairs based on new technology (other examples include the introduction of airplanes, the atom bomb, and long-range missiles). IW is defined as an attack on information systems for military advantage using tactics of destruction, denial, exploitation, or deception. The information cycle is vulnerable to these tactics at each step from information gathering to data entry to data transmission to information processing to information dissemination. Current research is searching for robust solutions at each step in the information cycle, but the problem is systemic in that for every new solution, a new threat is developed.

The rise of IW is linked to widespread diffusion of information technology. The most important enabling feature of the diffusion of information technology is declining cost. Since the 1950s, costs have declined 94% every five years, and most experts expect this trend to continue.

The IW threat will continue to grow at the expense of the cyber masses because entry costs are low and decreasing, leading a large number of foreign governments to organize strategic IW organizations within their military. A second feature of IW is that as the technology becomes less expensive, it becomes more efficient to decentralize away from a hierarchical command structure such as is traditional to military tradition.

Information systems are so critical to military operations that it is often more effective to attack an opponent's information systems than to concentrate on destroying its military forces directly. There is a perception within military circles that control of information may become more important than air superiority was in previous wars. This has lead to a reevaluation of military doctrine referred to as a revolution in military affairs (RMA).

An RMA is a major change in the nature of warfare brought about by the innovative new application of new technologies that, when combined with dramatic changes in military doctrine and operational and organizational concepts, fundamentally alters the character and conduct of military operations.

The United States is potentially vulnerable to IW attack because it is more dependent on information systems than any other country in the world. For example, in the United States, 99% of all military communications is carried over civilian infrastructure, thus intermingling military and civilian targets. In a civilian context, the quality of life of our most basic needs is dependent on automated information-management systems.

The U.S. Department of Defense (DoD) has budgeted billions of dollars to IW, and all the military services have formed distinct IW organizations, which are drafting IW military strategies. In January 1997, the Defense Science Board within the Pentagon released a task force report warning of U.S. vulnerability to an "electronic Pearl Harbor," which puts the cyber masses at great risk with a lot to lose.

The Defense Advanced Research Projects Agency (DARPA) is funding millions of dollars worth of research to develop an "electronic immune system" that will provide some level of protection to the cyber masses against IW attacks. The Pentagon already spends $8 billion a year to protect its information military systems.

A presidential commission was formed by Executive Order 13010 to issue recommendations on how to best protect the cyber masses from IW. Eight critical national infrastructures were considered so vital that their incapacity or destruction would have a debilitating effect on the defense and economic security of the United States. These eight critical national infrastructures as listed by the executive order are:

1. Electric power system (see sidebar, "Electric Power System Vulnerabilities")
2. Gas and oil storage and transportation
3. Telecommunications
4. Banking and finance
5. Transportation
6. Water-supply systems
7. Emergency services (including medical, police, fire, and rescue)
8. Continuity of government services (including federal, state, and local government services)

ELECTRIC POWER SYSTEM VULNERABILITIES

Nationwide rolling blackouts could have a devastating impact on the economy, but experts also fear that the stress being placed on the nation's power grid could make it more susceptible to disruptions from hackers. In California's Silicon Valley, large Internet data centers have been blamed for stressing the region's power grid beyond what its Korean War–era design can handle. Now, other states, including Oregon, Utah, and Washington, are preparing for possible rolling blackouts.

From a cybersecurity perspective, the electric power grids in the West are now more fragile, and margins for error are significantly less. With diminishing margins and power reserves, the probability for cascading catastrophic effects is higher.

The recent power shortages come as the Critical Infrastructure Assurance Office (CIAO) of the U.S. Department of Commerce delivered to Congress the first status report on private-sector efforts to bolster cyberdefenses for systems that run critical

→

sectors of the economy. Although progress has been made in improving information sharing, officials acknowledge that they still know very little about how failures in one sector could affect other sectors.

In the context of broader infrastructure assurance, the scale and complexities of the energy infrastructure and their impact on infrastructure security and reliability are not fully understood. The energy industry continues to be the target of Internet-based probes and hacker attacks that seek to exploit known vulnerabilities in off-the-shelf software and systems that are increasingly being used to control and manage the power grid.

Likewise, the sector continues to fall victim to poor personnel security practices, ports, and services that are open to the Internet; outdated software without current security patches; and improperly configured systems. With the system teetering on the brink of collapse, it becomes easier for a small incident to have a wide impact. For instance, if someone were to find a way to force the shutdown of a single power plant or a section of the power grid, the results would be much more devastating, because there is not enough reserve capacity to take up the slack.

In addition to the technical risks, the publicity generated by the recent crisis in California, and the possibility that hackers may try to exploit known vulnerabilities, there exists the possibility of making a bad situation worse. One risk with a situation like this is that it exposes the flaws of the system to public scrutiny. It shows everyone how vulnerable the cyber masses' economy is to a power disruption. Like it or not, there are people in the world who pay attention to such revelations.

Anytime the visibility of a system is raised, it acts as an attack magnet. It is recommended that companies, particularly utility companies, treat the power crisis as a signal to begin stepping up network monitoring and security operations. The link between the stress level on the power grid and its vulnerabilities act like blood in water to a shark. Hackers smell weakness and a chance for their 15 minutes of fame.

Electric companies have made significant progress in stepping up their security preparedness and have also set up information sharing and analysis centers to enable system administrators to share information with the FBI's National Infrastructure Protection Center. When a transmission system is stressed, the system operators and security coordinators operate at a heightened level of alert so they can quickly address and return the transmission system to normal from any situation that may occur. The electric system can withstand sudden disturbances such as electric short circuits or unanticipated loss of system elements. This was the case decades ago, and it is still true today.

The U.S. government should face the ethical consequences of the new global battleground now before a crisis arises by having a declarative policy concerning IW attacks. During the Cold War, the United States used a policy of strategic nuclear deterrence, warning that any nation that attacked the United States could expect total destruction in return. It is commonly believed that this policy of deterrence was successful, but is impossible to prove. By analogy, analysts have wondered if a similar strategy might deter IW attacks on the U.S. national information infrastructure (NII). For a strategy of deterrence to work the following must hold:

- The incident must be well defined.
- The identity of the perpetrator must be unambiguous.
- The will and ability to carry out a deterrence strike must be believed.
- The perpetrator must have something of value at stake.
- The deterrence strike must be controllable.

This strategy of deterrence must be measured in the context of the inherent vulnerability of large technologically based systems. In what has been called the "complex-system issue," the axioms are

- Complex systems fail in unpredictable ways from causes that seem to be minor and, often, obvious flaws in retrospect.
- The failure of a complex system may be exceptionally difficult to discover and repair.
- Complex systems fail at inopportune moments—usually during demanding system use when the consequences of failure are highest.

It must be possible to determine if an event involving one of the United States' vital infrastructures is the result of an accident, criminal attack, isolated terrorist incident, or an act of war. The damage to the cyber masses from an event may be the same regardless of the cause, but the cause of the event will determine the jurisdiction and nature of the response from the U.S. government. Possible jurisdictions include private industry, the FBI/Department of Justice, CIA/National Security Agency (NSA), or DoD; possible responses range from doing nothing to a nuclear retaliatory strike.

Ethical Challenges of IW to Prevent Cyber Masses' Losses

This section analyzes the most significant ethical questions of IW as a new form of warfare. Many of the questions have been raised before in previous contexts, but the unique characteristics of IW bring urgency to the search for new relevant answers.

This analysis is also pertinent to other military situations generally referred to as operations other than war (OOTW), such as peacekeeping missions, preludes to conflict, alternatives to conflict, sanctions, and blockades. For example, in an IW analogy to the U.S. blockade of Cuba during the Cuban missile crisis, there are IW techniques (jamming and denial-of-service attacks) that could be used to block and, thus, isolate rogue nations from international communications without circumventing physical sovereignty—much in the same way the British decided to sever all transatlantic telegraph cables that linked Germany to international communications at the outset of World War I.

What Constitutes an Act of War in the Information Age?

The nation-state combines the intangible idea of a people (nation) with the tangible construct of a political and economic entity (state). A state under international law possesses sovereignty, which means that the state is the final arbiter of order within its physical geographical borders. Implicit to this construct is that a state is able to define and defend its physical geography. Internally, a state uses dominant force to compel obedience to laws, and externally, a state interacts with other states, interaction in either friendly cooperation, competition, or to deter and defeat threats.

At the core view of any nation-state's view of war should be a national information policy that clearly delineates national security thresholds over which another nation-state must not cross. This national information policy must also include options that consider individuals or other non-state actors who might try to provoke international conflicts.

Increasingly, the traditional attributes of the nation-state are blurring as a result of information technology. With IW, the state does not have a monopoly on dominant force, nor can even the most powerful state reliably deter and defeat IW attacks. Non-state actors attack across geographic boundaries, eroding the concept of sovereignty based on physical geography. With the advent of the Information Age, the United States has lost the sanctuary that it has enjoyed for over 200 years. In the past, U.S. citizens and businesses were protected by government control of our air, land, and sea geographical borders, but now, an IW attack may be launched directly through (or around) these traditional geographical physical defenses.

War is armed conflict between nation-states. Historically, war has been a legal status that could be specified by declaration or occur by way of an attack accompanied by an intention to make war. The modern view of war provides a new look at the tradition of a just war, *jus ad bellum*, (when it is right to resort to armed force) and *jus in bello*, (what is right to do when using force). The six requirements of *jus ad bellum* were developed by Thomas Aquinas in the 13th century:

1. The resort to force must have a just cause.
2. It must be authorized by a competent authority.
3. It is expected to produce a preponderance of good over evil.
4. It must have a reasonable chance of success.
5. It must be a last resort.
6. The expected outcome must be peace.

There are two requirements for *jus in bello:* the use of force must be discriminate (it must distinguish the guilty from the innocent), and the use of force must be proportional (it must distinguish necessary force from gratuitous force). The application of just war reasoning to future IW conflicts is problematic, but there is a growing voice saying there is a place for the use of force under national authority in response to broader national security threats to the values and structures that define the international order.

Applying one aspect of just war reasoning to IW is the problem of proportionality. It is impossible to respond to every IW action, because there are too many. At what threshold in the lives of the cyber masses and their money, should the United States consider an IW attack an act of war?

Article 51 in the United Nations Charter encourages settlement of international disputes by peaceful means. However, nothing in the charter impairs the inherent right of individual or collective self-defense if an armed attack occurs.

NOTE

Infringement of sovereign geographical boundaries by itself is not considered an armed attack. Experts do not equate "use of force" with an "armed attack." Thus, certain kinds of data manipulation as a result of IW that are consistent with use of force would not constitute an armed attack under Article 51.

On the other hand, Article 41 of the United Nations specifically states measures that are not considered to be an armed attack: complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications. IW might still be considered an act of war, however, if fatalities are involved.

If data manipulation is such that the primary effects are indistinguishable from conventional kinetic weapons, then IW may be considered an armed attack. The paradigm shift is that weapons are devices designed to kill, injure, or disable people or to damage and destroy property and have not traditionally included electronic warfare devices.

What are the ethical implications of the blurring distinction between acts of war from acts of espionage from acts of terrorism? Let's take a look.

Ethical Implications

It is important to be precise in what the cyber masses identify as a crime and what they identify as an act of war. An armed attack as stated in Article 51 contemplates a traditional military attack using conventional weapons and does not include propaganda, information gathering, or economic sanctions. Espionage is a violation of domestic, not international, law.

The threat analysis section of the 1997 Defense Science Board Report indicates that a significant threat includes activities engaged on behalf of competitor states. This introduces the new concept of low-intensity conflict in the form of economic espionage between corporations. In the age of multinational corporations that view geographical boundaries and political nation-states as historical inconveniences, should economic warfare between multinational corporations involve the military?

The new IW technologies make it difficult to distinguish between espionage and war. If espionage is conducted by computer to probe a nation's databanks and military control systems, when is it an act of war versus an act of espionage? Does it depend on whether the intelligence was passively read versus information actively destroyed in battle or manipulated? Does it depend on whether the intelligence was used for military advantage or for political or criminal advantage? Does the answer depend on whether a state of war exists?

A different scenario is modifying internal computer software (via viruses, trojan horses, or logic bombs) or hardware (chipping) before shipment to cause an enemy's computer to behave in a manner other than they would expect. During peacetime, gaining entry to a computer's internal operating system could be considered a criminal offense or act of espionage, despite the fact that the action in question took place before the enemy had acquired ownership of the computer. Is this prudent preparation for IW or is this a hostile action that could precipitate a war? If the computer hardware chip is commercially manufactured and altered, what are the legal and ethical implications for a company inserting internal hardware hooks in cooperation with national security at the request of the government—especially if the company has international sales? Finally, is IW a potential step that might lead to an escalated conventional military conflict that could have been avoided by other means?

Can IW Be Considered Nonlethal?

Nonlethal weapons are defined as weapons whose intent is to nonlethally overwhelm an enemy's lethal force by destroying the aggressive capability of their weapons and temporarily neutralizing their soldiers. Nonlethal most often refers to immediate casualty counts, not downstream collateral effects.

In response to the power of cyber masses' opinion and instant global media coverage, the U.S. military has begun to develop a new kind of weaponry designed to minimize bloodshed by accomplishing objectives with the minimum use of lethality. This weaponry includes sticky foam cannons, sonic cannons, and electromagnetic weapons— which effectively temporarily paralyze the enemy without killing them.

Is it more ethical to use a sophisticated smart bomb precisely targeted to kill 30–40 soldiers immediately or is it more ethical to choose a nonlethal weapon that has the same tactical effect with no immediate casualty count but an indirect collateral effect of 600–700 cyber mass deaths? Ethically, the function of the target against which the weapon is used and the existence or lack of a state of war determines one ethical framework for analysis. For instance, disabling the electronics of a fighter plane or air defense radar during wartime is the goal of a large investment in electronic warfare equipment by the United States and is considered fair and ethical. However, disabling the electronics of a civilian airliner or air traffic control, during either peacetime or wartime, violates the principles of discrimination of combatants and proportionality of response and is considered unethical and a act against the cyber masses.

Is It Ethical to Set Expectations for a "Bloodless War" Based on IW?

As nonlethal weaponry of all types (especially IW weapons) advance from novelty to norm many potential pitfalls will need to be faced. The most important of these is the expectation that such weapons will ultimately allow wars to be fought without casualties.

Nonlethal military capabilities are not new, although IW weapons are the newest weapons in the nonlethal arsenal. Military forces have used riot-control chemical agents, defoliants, rubber bullets, and electric stun weapons for decades. As U.S. military forces are involved in missions that require extended direct contact with civilians (Somalia, Bosnia), force can no longer be viewed as either on or off, but rather as a continuum with nonlethal weapons on one end and nuclear devices on the other end. In more traditional conventional warfare, IW attacks to disrupt, deny, and destroy C4I capabilities (command, control, communication, and computer intelligence) are a core part of military tactics and strategy. If IW weapons can be used to remotely blind an opponent to incoming aircraft, disrupt logistics support, and destroy or exploit an adversary's communications, then many of the problems associated with the use of ground forces for these missions can be avoided.

It is important to point out that although nonlethal weapons are not meant to be fatal, they can still kill if used improperly or against people particularly susceptible to their effects. Because these technologies are potentially lethal in these circumstances, the term *nonlethal* has not been universally accepted within the U.S. military. For example, the U.S. Marines Corps uses the term *less lethal* to imply that there is no guarantee of nonlethality.

Asserting that IW will ultimately allow future wars to be fought without casualties is a widespread misconception likely to prove counterproductive and even potentially dangerous to the cyber masses. First, all nonlethal weapons are not equally applicable to all military missions. Second, overselling of nonlethal capabilities without providing a context can lead to operational failures, deaths, and policy failure. Third, unrealistic expectations about nonlethal weapon capabilities inhibit their adoption by military forces who need to build confidence in these weapons.

There is a large asymmetry in global military power when comparing the United States to other nation-states. In 1994, the U.S. DoD budget exceeded that of

Russia, China, Japan, France, and Great Britain combined. This asymmetry makes it unlikely another nation-state would challenge the United States in a direct high-technology conventional war, except in circumstances that cyber masses should not depend on (incredible miscalculations or ignorant dictators, which were both present in the Gulf War.

Despite the luxury of a bumbling opponent, the success of the Gulf War has led the U.S. citizenry to expectations of low casualties in all future conflicts. These expectations go against two cardinal rules of military strategy: (1) you do not plan to refight the previous war and (2) the future battlefields cannot be dictated by the United States. The next battlefield for which the U.S. DoD is preparing is a global battlefield with weapons of IW targeting the civilian infrastructure. Even in this scenario, military and civilian casualties will be likely from either primary or secondary effects of IW attacks.

Is It Ethically Correct to Respond to IW Tactics with IW Tactics?

If the United States is attacked by IW weapons, how should the U.S. government respond? By changing perspectives from defense to offense, what is in the U.S. arsenal to wage IW against an adversary:

- Offensive software (viruses, worms, trojan horses)
- Sniffing or "wiretapping" software (enabling the capture of an adversary's communications)
- Chipping (malicious software embedded in systems by manufacturer)
- Directed energy weapons (designed to destroy electronics but not humans and buildings)
- Psychological operations (sophisticated and covert propaganda techniques)

A strategy that uses these weapons in various combinations has the potential to replace conventional military forces. The questions remain: is it ethically correct for the United States to defend its security interests by resorting to the same IW tactics that are used against it? Should information attacks be punished by information counterattacks? The options include maintaining the United States' superpower status at all costs, covertly listening to their adversaries but not actively disrupting operations, or contracting mercenaries, who are not officially affiliated with the U.S. government, to do their dirty work.

Cracking computers to deter and punish computer cracking erodes any moral basis the United States has for declaring the evils of IW warfare. It is also harder to predict secondary effects because of the globalization of systems. Retaliation may produce effects ranging from nothing to being counterproductive through destruction of U.S. interests. A nation-state or non-state actor that sponsors an attack on the U.S. NII might lack an NII of their own for the United States to attack in punishment and, thus, not be intimidated by a U.S. IW deterrence strategy.

Short of an official declaration of war, nation-states may seek UN Security Council action authorizing "all necessary means" even in the absence of an armed attack in cases of any threat to peace, breach of peace, or act of aggression. Every breach of international law creates a duty to pay for loss or damages; nation-states may seek recompense under "state responsibility doctrine." In addition to recompense, retribution in the form of proportional countermeasures are authorized when an IW attack that does not involve the use of force violates international law. IW may violate multiple international laws depending on the scenario, including the following:

- UN Convention on Law of the Sea (prohibits unauthorized broadcasts from the high seas)
- International Telecommunications Convention of 1982 (requires nations to avoid "harmful interference")
- INTELSAT Convention (satellite communications for nonmilitary purposes) [1]
- INMARSAT (maritime satellite communications for "only peaceful purposes")
- Chicago Convention (refrain from endangering safety of flight)

According to DoD Policy Directive 5100.77, U.S. military forces are bound by law to follow the rules of engagement of the specific conflict as follows: "The Armed Forces of the United States shall comply with the law of war in the conduct of military operations and related activities, however such conflicts are characterized." The problem is that there are no characterized rules of engagement for IW conflicts, which can take the form of isolated operations, acts of retribution, or undeclared wars.

The most serious problem for using IW retaliation to counter IW attacks is that adversaries could counter or copy IW capabilities. Every breakthrough in offensive technology eventually inspires a matching advance in defensive technology, thus escalating an IW weapons race.

A last issue related to retaliation is the ethical dilemma faced by the intermingling of the military and civilian sides of society. Given the uncertainty of deterrence and identifying the enemy, is the most ethical strategy for retaliation one that attempts to separate the military from civilians and, in so doing, diminishes their impact, which potentially prolongs the duration of the conflict, or a strategy that attempts to minimize lethality and duration but deliberately targets civilian systems?

Can Protection from IW Take Place in the United States Given Our Democratic Rights?

How much government control of the U.S. NII is permissible in a free society? Most of the IW technology is software, which is easy to replicate, hard to restrict, and dual-use by nature (having civilian and military uses). The 1997 Defense Science Board report states that the DoD is "confused" about when a court order is required to monitor domestic communications. This raises basic questions about the constitutional and ethical balance between privacy [2] and national security in a new IW context.

A "Big Brother" approach that places all of a nation's telecommunications under a single government jurisdiction is improbable given the diffusion and complexity of technology and the shrinking size of government. Most systems were built to serve commercial users who will vehemently object to unfunded mandates (taxes) and new requirements not driven by business demand (CLIPPER chip encryption and key escrow accounts). Regardless, it is critical to the future security of the United States that the cyber masses find a way to protect their infrastructure from IW attack and have contingency plans for potential IW crises. If an IW attack is detected and the enemy identified, but the United States is unable to react promptly because of bureaucratic inefficiency or indifference from private industry, it may be too late to react at all.

Current political discussion has floated tax incentives and direct subsidies to promote industry cooperation. In a related matter that may provide a precedent, the government has pledged to provide telephone companies with at least $1.2 billion to ensure that FBI officials can access telephone conversations over digital circuits (as opposed to accessing telephone conversations over analog circuits, which is technically much easier).

THE DESTRUCTION OF PERSONAL ASSETS IN IWS

The Mounties always get their man—or, when it comes to hackers, their boy. In 2000, Canadian cops announced the arrest of a Montreal-area 15-year-old for disabling CNN's Web site. His father was also nabbed, on unrelated charges of plotting to assault a business associate. The teen suspect, who was identified only by the hacker handle Mafiaboy, allegedly bragged about his exploits in online chats. He was not what one would call a genius. Mafiaboy was charged with two counts of mischief to data and faces two years' detention plus a $786 fine. While awaiting trial, he could not enter any public space that hosts networked computers.

The CNN.com incident was part of a rash of denial-of-service attacks that crippled Yahoo!, eBay, and other Internet titans, leading to a manhunt that stretched throughout the United States, Canada, and Germany. The international dragnet was spurred by damage and destruction of personal and corporate assets estimated at up to $2.3 billion.

Critics charge that companies and prosecutors regularly inflate such numbers and that the Mafiaboy case is no exception. If you're a law enforcement organization, it makes the crime look more serious. If you're a company, it allows you to get more money from insurance (see sidebar, "Hacker Insurance"). If you're the press, it makes the story more sensational.

HACKER INSURANCE

In the increasingly competitive hacker insurance market, American International Group (AIG) is making an offer it hopes prospective clients won't refuse: a free, comprehensive security assessment. AIG, the largest commercial insurance underwriter in the United States, hopes the free on-site security check—which ordinarily can cost tens of thousands of dollars—will encourage more companies to buy insurance coverage from it. AIG is one of the biggest players in a swarm of underwriters and brokers who are rushing into the hacker insurance market, a sector that the Insurance Information Institute estimates could generate $6.9 billion in annual premiums by 2009.

The insurers' sales efforts are being aided by highly publicized events such as the "Anna Kournikova" worm that tied up mail servers around the world. Insurance industry officials indicate their business is doubling every 7 to 13 months, as worries about hacking increase and more information technology professionals realize their companies' standard insurance policies don't cover risks incurred by their Internet-based businesses.

Cyber masses aren't used to spending money on this. The cost of the insurance application in the past included (for almost everyone) an on-site security assessment that would cost upward of $60,000, regardless of whether you bought the insurance.

To help convince qualified prospects (applicants must be seeking $6 million or more in coverage) to buy insurance, AIG pays independent security firms Global Integrity and Unisys to do the on-site assessments. The firms do external probes and "ethical hacking" of a prospect's Web site, as well as a three-day, on-site analysis to determine what types of security problems the company faces.

At the end of the assessment, if a prospect decides not to buy AIG's coverage, the company can keep the security report and assessments as AIG's gift. Although AIG's assessment is free, some competitors expressed skepticism. AIG's offer may create a false sense of security among insurance buyers. Security is not a product; it's a process.

WHAT'S COVERED

Companies interested in hacker insurance can buy coverage either as a package or a la carte. Some policies only pay for risks associated with loss or misuse of intellectual property. Others cover liability for misuse of a company's site by a third party, or damage caused by an outside hacker.

Premiums are generally based on a company's revenue, as well as the type and amount of coverage being sought. Rates vary. A package policy that covers a range of risks, including liability, loss of revenue, errors and omissions, and virus protection,

→

can cost from $10,000 to $54,000 per year (or more) for each million dollars of coverage in the policy.

Given the range of costs and coverage, industry officials warn potential buyers to be wary. Some policies cover only the amount of net income lost due to hacking. A better choice for some companies may be coverage for lost revenue.

Numerous variables can affect premiums. Just as a buyer of auto insurance can choose a high deductible to lower the premium, hacker insurance buyers can choose different waiting periods before coverage begins. For instance, a policy that begins paying for business losses just four hours after a hacker shuts down a site may cost more than a policy that begins paying after 24 hours of downtime. These waiting periods, called "time element deductibles," are variable and depend on the kind of business being covered and the amount of risk a business may face.

Companies can also get substantial discounts on their policies if they have managed service contracts with an insurer-certified security firm. Security assessments are critically important for both insurers and insurance buyers. Hacker insurance is such a new product that there are no reliable actuarial tables to determine rates. Therefore, insurance companies rely heavily on the assessments to help them determine the amount of risk they are taking on with a given company. For the companies seeking insurance, assessments should help them find (and immediately fix) holes in their defense systems.

Stiff Competition

Underwriters competing with AIG (the Chubb Group, Fidelity and Deposit Companies, St. Paul Companies, Lloyd's of London, and Wurzler) are rolling out a fleet of new products and alliances to help them gain market share. Chubb recently announced new coverage designed for online banks, brokerages, and insurance companies. Wurzler has joined with Hewlett-Packard to market its products to a select group of HP's clients.

Insurance brokers and security firms are teaming up to sell branded products and services. Marsh & McClennan Companies, the world's largest insurance brokerage, is selling insurance provided by AIG, Chubb, and Lloyd's. The brokerage relies on internet security systems to do its security assessments. Counterpane Internet Security has allied with brokers Safeonline and Frank Crystal & Co. to provide its clients with special policies underwritten by Lloyd's.

It's a wildly growing market, and its primary underwriters are AIG, Fidelity and Deposit, and Wurzler. Hacker insurance has been a small market because people were waiting for e-commerce to hit. Well, now e-commerce has hit.

Insurers are finding a ready market for their products, because companies with Internet operations are increasingly under attack. A survey conducted in 2004 by the

→

FBI and the Computer Security Institute, an association of computer security personnel from the private and public sectors, found that from March 2002 to March 2003, 32% of the 1,085 governmental agencies and businesses that responded indicated that they experienced denial-of-service attacks. Viruses are also wreaking havoc. Losses from 2000's "Love Bug" virus were estimated to be as high as $20 billion.

AIG's move to lower the cost of obtaining hacker insurance shows that the market is beginning to mature, according to industry experts. Security analysts hope it will encourage more Net companies to get insurance coverage.

Companies need to understand that getting hacked is not only an inconvenience. Anything Internet-facing is a point of vulnerability. Companies can be attacked directly or they can be used to attack someone else. There's real exposure and liability. They need to reduce their risk, and the only way to do that is through proper insurance.

Pricing cyberintrusions is pretty much a guessing game. If a burglar steals your television set, you know what its replacement value might be, but what's the value of the time of all the people who had to drop their work and deal with this hacker nonsense? More tangential costs are also often tabulated; the $5.6 billion figure associated with recent attacks, calculated by the Yankee Group, includes the expense of security upgrades, consulting fees, and losses in market capitalization from tumbling stock prices.

The implication is that companies wouldn't have had to spend the money if they never had a problem. That's like saying you don't need to get a lock for your front door unless somebody breaks in.

Fair Punishment

Inflated estimates can skew jail terms. A formula should be devised to calculate the severity of hacks. The question is, how serious a societal harm has been done in the hands of these companies, without any real checks or balances? If the FBI is going to punish people by sending them to prison, they probably don't want to send them to prison for something that's just a nuisance.

In one famous case, an editor at the computer-security webzine *Phrack* was charged with publishing a document stolen from BellSouth's network. Prosecutors valued the 13-page paper at $80,550, which included the $42,000 cost of the computer it was typed on, $7,000 for the printer, and $7,300 for a "project manager." It was revealed at trial, however, that BellSouth sold a nearly identical document to the public for just $14 per copy.

SHORT- AND LONG-TERM PERSONAL ECONOMIC IMPACT ON CYBER CITIZENS

Cyberattacks cost U.S. organizations and their cyber citizens $600 million in 2003—more than double the average annual losses for the previous three years. The study, released by the San Francisco–based Computer Security Institute (CSI) and the San Francisco FBI Computer Intrusion Squad, found that 95% of survey respondents detected some form of security breach in 2003.

Based on information from 617 of CSI's member organizations, 75% reported serious security attacks, including theft of proprietary information, financial fraud, system penetration from outsiders, denial-of-service attacks, and sabotage of data or networks. This figure, up from 67% in 2001, didn't include data from common security problems caused by computer viruses, laptop theft, and abuse of Internet access by employees.

According to the report, 79% of respondents confirmed that they sustained financial losses from security attacks, but only 47% said they were willing and able to quantify these costs. The figures are based on responses from 1,087 computer security practitioners in 617 U.S. corporations, government agencies, financial institutions, medical institutions, and universities.

The $600 million in verifiable losses claimed by respondents was more than twice the average annual total of $473 million reported from 2001 to 2004. Eighty respondents reported $100.1 million in losses from theft of proprietary information, and 97 organizations listed $90 million in losses from financial fraud.

CSI indicates a continuing trend in the study—that computer security threats to large corporations and government agencies come from both inside and outside the organization. Whereas media reports often focus on outside computer crackers, 85% of respondents were worried about disgruntled employees. Sixty-five respondents indicated that they suffered $51 million in damages from sabotage of data or networks, compared to a combined total of $65 million for previous years.

For the sixth consecutive year, 63% of respondents identified their Internet connection as a frequent point of attack, compared with 36% who cited internal systems as the target. The short- and long-term personal economic impact on cyber citizens continues to be staggering.

Unauthorized access and security attacks are widespread. The private sector and government organizations must increase their focus on sound security practices, deployment of sophisticated defensive technology, and adequate training and staffing of security managers.

THE VIOLATION OF PRIVACY DURING INFORMATION WARS

Privacy—who could possibly be against it? Not IBM, which has vowed to yank all its ads from Web sites that fail to post a clear privacy policy. Not America Online, which promises never to disclose information about members to "outside companies." Certainly not Microsoft, which in 1999 threw its weight behind a plan that could one day let people skip automatically past sites that don't meet their privacy standards. The biggest collectors of information, it seems, are suddenly in the forefront of the campaign for our right to be left alone.

Privacy protection is good for business, but it may not be not quite that simple. True, millions of Americans are wary of the Internet, and surveys suggest that many are hanging back because of confidentiality concerns.

However, the recent frenzy of corporate initiatives is only partly about building public trust. It's also about fending off legislation. Corporate America is mobilizing against the threat of a broad federal privacy-protection law. In particular, businesses are disturbed by one likely element of such a law: a subject access provision that would allow citizens to find out what companies know about them and how the information is being used.

To comply with such a measure, corporate information systems would have to be retrofitted to serve a purpose for which they weren't designed—a vastly expensive undertaking that worried executives liken to the year 2000 problem. The technological costs, however, could be exceeded by the psychological costs.

Junkbusters

If subject access becomes law, Americans will be stunned to discover how much data large corporations have on them. People are going to be horrified. So far, the United States has addressed the subject on a case-by-case basis. The confidentiality of video rentals is protected, for example, because a reporter got hold of Robert Bork's rental records during the fight over his failed nomination to the Supreme Court. Otherwise, corporate lobbyists have sold republican and democratic leaders alike on their view of the Internet economy as a tender, if vital, young thing needing protection from the regulatory mechanisms of the past.

The market can do the job. In addition, companies are banding together to develop privacy guidelines, hoping to show that they can regulate themselves. That premise, however, is under mounting attack on two fronts, domestic and foreign.

The immediate pressure is coming from Europe. A European Union (EU) privacy directive that took effect in October 2004 not only includes subject access but also requires that, when soliciting information from people, companies clearly spell out what they intend to do with it. This concept is anathema to many large

U.S. companies. Accustomed to collecting data for hazy purposes (a "personalized experience"), businesses reserve the right to discover more specific uses or sell the information later on.

The most annoying element of the EU directive, as far as U.S. corporations are concerned, is a ban on transborder shipment of data to countries that don't offer "adequate" privacy guarantees. The Sabre Group, a Texas-based airline-reservation network, is fighting in Swedish court for the right to maintain in its global data bank such facts as a passenger's wheelchair use or preference for kosher meals. Prodded by Sabre and other large information-oriented companies, the U.S. government is trying to convince European officials that the argument isn't really over the degree of privacy protection, but over two different "cultural perspectives." The Europeans have gone to ridiculous extremes, creating privacy commissions and "privacy czars" to deal with such trivialities as L. L. Bean's decision to send out a catalog of their home products as opposed to their clothing products. Literally interpreted, the EU directive would bar a traveling American business executive from flying home with the names and phone numbers of European clients in his laptop.

Double Standard

Such fears are overwrought, but European officials point to deep historical reasons (including Nazism) for their view of privacy as a basic human right. The White House is not in any position to cut deals on that, any more than the British are in a position to cut deals on the U.S.'s First Amendment. But if Washington has to make concessions, U.S. multinationals could find themselves in the ticklish position of explaining why they have granted rights to Europeans that they are trying to withhold from Americans. The self-regulation concept has already suffered a series of embarrassments at home. In 1999, Microsoft was discovered to be collecting data on users who had expressly requested anonymity.

Privacy advocates agree that there are informal and technological fixes for many of the problems. Online privacy protection has the potential to become a significant industry in itself, but it will grow much faster with legal incentives. In the absence of sanctions, the privacy commissioner of Hong Kong claims that self-regulation amounts to putting Count Dracula in charge of the blood bank.

Oddly enough, the concept of subject access originated in the United States, with the Fair Credit Reporting Act of 1971. Credit companies have been living quite profitably with the rule for over 33 years.

Many of the same companies that have been battling against a federal privacy law have pressed Congress to enact more stringent copyright and patent laws. They're only against regulation when it's something they don't like.

THE INDIVIDUAL EXPOSED

On the Internet, goes the saying, nobody knows you're a dog. If that ode to online anonymity was once true, the notion seems laughable today. The Internet is now more like an unlocked diary, with millions of consumers divulging marketable details of their personal lives, from where they live to what they eat for dinner. Operators of sites on the World Wide Web collect and sell the information or use it to lure advertisers. Software tracks the sites you visit and the pages that catch your eye. If you were a dog, online snoops would soon learn that you're a collie who plays a mean game of Frisbee catch and likes your kibble moist.

No one is immune. Online databases bulge with facts on millions of Americans. "Spammers" cram your emailbox with ads. Continuous loopholes in Netscape Navigator and Microsoft Explorer give Web administrators direct access to the hard disk of any browser user visiting their site.

Businesses recognize the Web's potential as a shopping mall, but because of concern over consumer privacy, many stores in that shopping mall have been forced out of business. It doesn't help matters that many Web sites don't reveal how they intend to use the information collected or whether it might be shared. In a recent survey by the Boston Consulting Group, more than 77% of online users worried more about offering up private facts online than they did via phone or mail—so they often refused or gave false information. Mounting user fears prompted the Federal Trade Commission (FTC) to hold a four-day public workshop recently to determine whether the government should step in. Congress is examining the issue, too; several measures to govern the use and sale of personal data, such as Social Security numbers, are pending.

Facing possible regulation, online companies vowed during the workshop to help individuals preserve their anonymity and decide whether to reveal personal details. After all, a pro-consumer stance is good for business. It is estimated that online consumer commerce will grow from 2001's $68 million to as much as $101 billion by 2005—if privacy is addressed, that is.

Of course, you can avoid keying in anything you consider private, but that would bar you from using quite a few sites, and abstinence is not always foolproof. Using a technology called "cookies," some sites, unbeknownst to you, can pick up the address of the site you most recently visited and the Internet service provider (ISP) or online service used and can log your movements within the site. Even companies that advertise there can drop cookies on your hard drive without your knowledge; some expire only after 2005.

Web users do have a few ways to deal with the cookie problem. Surfing through the Anonymizer hides your identity but slows you down to some degree. You can also program most popular Web browsers to accept or reject cookies before they are downloaded to your hard disk. Many shareware programs, which can be tried out before being purchased, can help you manage cookies (you might want to permit cookies from a personalized news product, for example) or cut them out entirely.

Our Private Information Is Everywhere!

None of these tools, however, will wipe out details about you that are stored in online databases ranging from telephone directories such as Switchboard and World-Pages to commercial reference services such as Lexis-Nexis, CDB Infotek, and Information America. Résumé banks, professional directories, alumni registries, and news archives can all be harvested, as well.

Resourceful thieves can exploit these online caches. The Delaware State Police nabbed a couple recently who had obtained birth certificates and drivers' licenses in others' names (thus enabling them to open bank accounts and get credit cards) using information gleaned from sources that included the Internet. Going online made it much easier for them to get at some of the more personal information.

Eight major reference services announced an agreement at the FTC workshop to prevent the misuse of nonpublic data, such as the name, address, and Social Security number found at the top of a credit report. A law enforcement agency, for example, might see all of the data, but a commercial enterprise might not see the Social Security number.

NOTE

The Fair Credit Reporting Act restricts dissemination of data in the body of a credit report (such as credit card accounts, car loans, or mortgages), but does not cover the material at the top.

Much of the material in online databases is culled from public files such as property tax records and drivers' license rolls. That raises questions about the quality of the data. Databases are notoriously inaccurate, yet major institutions use such services to judge, for example, fitness for employment and insurance. Privacy advocates say consumers should be told if any personal facts are being sold and should have the right to dispute errors in the databases. In their proposed privacy guidelines, however, reference services agreed merely to tell people the "nature" of the data held on them.

Privacy advocates also argue that consumers should be able to opt out of junk email, or spam. America Online, the largest online service in the U.S. says that up to 34% of the 19 million email messages its members receive each day are junk and that spamming is members' number 1 complaint. Although all major online services and ISPs prohibit spamming and use filtering programs to weed it out (several have won injunctions barring spammers from their networks), the filters don't always work. Sleazy marketers often use fake return addresses that are nearly impossible to track down. The FTC recently vowed to prosecute perpetrators of fraud and deception, soliciting the assistance of the Internet E-Mail Marketing Council.

The FTC recently gave online businesses and organizations six months to a year to make good on their promises to protect the privacy of online consumers. If that does not happen, the FTC will consider taking stronger steps to enable people to browse and buy confidently as if they were shopping at the local mall.

IDENTITY THEFT

Stolen identity [3]? It can ruin your credit. And that's just the beginning. When Dee Helus (named changed to protect her privacy) and her husband went to the bank in December to refinance their home, they thought it would be routine. After all, the couple, who live in Kansas City, Kansas, were refinancing with their existing mortgage lender and they prided themselves on their credit history. So it was quite a shock when the bank officer turned them down, pointing to their credit report, which listed numerous accounts in arrears.

It turns out that a woman in Illinois had applied for credit 55 times using Helus's name and Social Security number. In all, she had made purchases totaling $120,000, leaving a trail of unpaid debt that Helus is desperately trying to prove is not hers: a $61,000 loan for a mobile home, three car loans, credit card bills, and charges for a cellular phone and other services. The perpetrator torched her credit to the point where even the perpetrator herself was denied.

Helus is a victim of a crime of the 21st century: identity theft. It happens when one individual uses another's personal identification (name, address, Social Security number, date of birth, mother's maiden name) to take over or open new credit cards and bank accounts, apply for car and house loans, lease cars and apartments, and even take out insurance. The perpetrators don't make the payments, and the victim is left to deal with the damage: calls from collection agencies and creditors, the endless paperwork that results from trying to expunge fraudulent accounts from a credit record, and the agony of waiting to see if more phony accounts pop up. Meanwhile, the proliferation of black marks on a credit report can be devastating. Victims of identity theft are often unable to get loans. Some run into trouble applying for a job. A few have even been arrested after the thief committed a crime in the victim's name.

Many identity thieves use stolen personal information to obtain driver's licenses, birth certificates, and professional licenses, making it easier to get credit. Most victims don't even know how the criminals pulled it off. Data have been stolen from desk drawers in the workplace, mailboxes, job application forms, and the Internet. False identification cloaks a thief in anonymity, and the impostor can often use the alias for a prolonged period of time. Thieves typically have the bills sent to an address that is not the victim's, concealing the scheme for months, even years. Most victims aren't aware that their credit has taken a nose-dive until, like Helus, they apply for credit themselves or receive a call from a bill collector.

In the 1980s, criminals who wanted free plastic simply made up counterfeit credit cards with the correct number of digits. To thwart them, the industry instituted sophisticated security measures involving holograms and algorithms. Now criminals are taking advantage of what some see as the weakest link in the credit system: personal identity. There is nothing in the system that demands proof that you are the person you say you are. Personal identifiers are now, more than ever, a valuable commodity to criminals.

Although no single agency tracks identity fraud, statistics collected by the Government Accounting Office point to a growing problem. Trans Union, for example, one of the three major credit bureaus, indicates three-fourths of all consumer inquiries relate to identity fraud. Those inquiries numbered 855,255 in 2000; in 2004 there were 1,299,699. The costs of identity fraud can be very high: the Secret Service indicates losses to victims and institutions in its identity-fraud investigations were $5.2 billion in 2004, up from $1.8 billion in 2000. It's a problem that Congress finally addressed by making it a federal offense for anyone caught perpetuating identity fraud.

Most victims call the police, but in states with no statute, some police departments refuse to take a report because the law sees the victim in a case of identity fraud as the party that granted the credit (the bank or the merchant, for example), not the person impersonated. That's frustrating to the victims because they often need a report to prove they are not the bad guys.

Victims need proof because the attitude they often encounter when dealing with creditors is guilty, guilty, guilty. Every person Doyle Comfort (name changed to protect privacy) talks to has been skeptical, condescending, and hostile, and he is still trying to clean his credit report of 26 bounced checks written to stores in Arizona in 1997 on a bank account opened fraudulently in his name. That really aggravates Comfort, who has already been turned down for a mortgage. Victims often have to play detective, coming up with clues, leads, and even the basic evidence that a fraud has been committed. They have to do all the footwork themselves.

Typically, creditors ask an identity-theft victim to fill out an affidavit certifying he or she did not incur the debt. Some require much more: one collection agency told Helus it needed a copy of her driver's license, her Social Security card, her birth certificate, and any lease or mortgage contract from the past five years—all for an $87 cable bill. In the end, Helus neither paid the bill nor sent the copies to prove her innocence, opting to explain the $87 item on her credit report to future creditors. As with many victims of identity theft, sensitive documents were the last thing she wanted to send to a stranger.

The belligerence that victims encounter from some creditors is particularly irksome to those who suspect a creditor's negligence in the first place. Many creditors do not take the proper steps to verify the identity of the credit applicant. Dorothy Haskins (name changed to protect privacy) of Reston, Virginia, points to a credit-card application that started an impostor on a crime spree in her name. The application was preprinted with the impostor's name and address, but the impostor crossed off her own name (leaving her address) and wrote in Haskins name, Social Security number, and occupation. The bank gave the impostor a credit card with a $50,000 credit line, leading Haskins to ask, "Wouldn't a reasonable person say something is fishy here?" Bankers, meanwhile, insist they are on the ball. All the banks have systems that detect fraud. They have to modify them for every new scheme that comes up.

To make matters worse, two weeks after Haskins notified the bank that the account was fraudulent, the bank sold it to a collection agency, and she and her children started receiving threatening phone calls and letters. It didn't stop there. The card triggered an avalanche of preapproved credit offers to the phony Haskins mailbox: One different address on a credit account was all it had taken for one of the credit bureaus to switch Haskins credit-file address to the impostor's. They came to Haskins like candy. Some credit bureaus won't change a file address until three creditors report a new address, but a criminal on a spree can quickly cross that threshold.

It's not easy getting a credit report back on track. The credit bureau says contact the creditor, the creditor says contact the credit bureau, and the consumer just gets ping-ponged back and forth. The bureaucracy can be maddening: Helus recently received a letter from the credit bureau Experian saying it was reinserting a disputed item. The letter did not say which of the 25 accounts it referred to.

One of the few weapons victims have to protect them is a "fraud alert," which credit bureaus will put in consumer credit files. This notifies anyone who pulls the report that the subject is a victim of fraud and that he or she should be called to verify any credit application. The alert isn't foolproof.

Credit bureaus might want to step up their efforts at finding a solution before more aggrieved consumers turn to the courts. Recently, in Clarksdale, Mississippi, a man won a lawsuit against Trans Union for failing to clean up his credit report. The award: $7.8 million.

Meanwhile, the credit-reporting industry has formed a taskforce to tackle identity theft. Among solutions being considered are taking files of theft victims offline and sharing fraud alerts among credit bureaus more quickly. Individual creditors are also taking steps to stem their losses and prevent future ones. In San Francisco, Cellular One routinely flags suspect applications and compares details with credit reports. That's how Irene Cole (named changed to protect privacy) of San Francisco found out her identity had been compromised. Moreover, Cellular One alerted competitors in the area that they might be the next targets.

Identity theft is a crime that comes back to haunt its victims, and many are taking determined measures to prevent its recurrence. Helus and her husband have taken an unusual vow: when they have children, they will not get them Social Security numbers—even though that means no tax deduction. To her way of thinking, safeguarding her children's identity is far more valuable.

MONITORING PRIVATE AFFAIRS IN CYBERSPACE

Not being Prince Charles or Newt Gingrich, most of us give little thought to cell-phone eavesdropping. After all, who cares if someone overhears you telling your husband or wife you're stuck in traffic. Of course, if the conversation is of a sensitive nature, then one of your concerns is (or should be) the security of your phone.

Cellular service providers have a different security problem. Their great concern is service theft, through which criminals succeed in using a cell phone without paying for it. In the early days of cellular telephony, service theft mostly meant cloning. People with radio scanners would simply "sniff" the cellular frequency bands, pick up cell-phone identification numbers, and program them into other phones. That problem has been reduced by almost two orders of magnitude through the application of some thoughtful technology, but it has been replaced by other problems: subscription fraud (the same problem that bedevils issuers of credit cards) and the misapplication of service provider subsidies on handsets.

Subscription fraud has several forms: pretending to be another, real person; pretending to be a nonexistent person; and even just being yourself and pretending you intend to pay your bill. Subsidy fraud involves taking a phone whose cost has been heavily subsidized by a cellular carrier and activating it on a different carrier's network.

Solutions to these problems exist. However, the newest and best of them cannot be implemented on old handsets, so the technical situation is not without interest. Some of the solutions, particularly those used to fight subscription fraud, tend by their very nature to inhibit sales (after all, the idea is to eliminate deadbeats), which presents the executives of cellular companies with a dilemma. On the one hand, many of them need the revenue stream from a large number of subscribers to help them pay off the huge investments they made when they bid wildly for spectrum space back in 1995. On the other, they have no desire to be cheated.

As the practice of conducting serious business over the Internet continues to grow, other security issues will arise. In particular, someone conducting business on a cell phone needs to be confident of the identity of the other instrument's user. The technical solutions to be discussed here, such as radio frequency (RF) fingerprinting and authentication, do a good job of guaranteeing that the handset is what it claims to be, but they guarantee nothing about the person using it.

Several approaches are being pursued for user identification. The problem, in fact, is not finding solutions, but getting everyone to agree on which to use. To do banking over a cell phone, your bank, your cellular service provider, and your phone must agree on the same end-to-end solution. The phone companies, as an industry, must standardize that solution to drive mass-market end-user accessibility.

Analog Yes, Digital No

When it comes to eavesdropping, the situation is pretty simple. Analog phones are easy to bug; digital are hard. Although it is illegal to sell scanners in the United States today that are capable of receiving the frequency bands used for cellular telephony (824–849 MHz, 869–894 MHz, 1.85–1.91 GHz, and 1.93–1.99 GHz), older units that can receive them are readily available. Moreover, it is hardly rocket science to modify a new, compliant receiver to add the extra bands.

NOTE

The scanners are capable of receiving at least the lower bands; they have just been rigged to block them.

Lest anyone think that analog cellular telephony is an old, dead technology, as of June 2002, over 40% of the subscribers in the United States still used analog handsets, according to Boston's Yankee Group. Many who have dual-mode phones (capable of analog and digital operation) turn to the analog mode when roaming, especially in rural areas.

The latest figures from the Cellular Telecommunications Industry Association (CTIA), indicate merely that digital penetration today exceeds 80% but the CTIA counts dual-mode handsets as digital, so its number may not be so different from the Yankee Group's. Whatever the precise numbers, the message is clear: eavesdropping is not of only historical interest.

Digital phones, be they of the time- or code-division multiple-access (TDMA or CDMA) variety, are, unlike analog units, foolproof against eavesdropping by ordinary mortals. Would-be listeners-in, for one thing, have to know what system they are trying to tap into, because TDMA and CDMA are utterly different. For TDMA, what can be snatched out of the ether is a digital data stream representing one side of each of three multiplexed conversations. Eavesdroppers need to lock onto the correct time slot to get the conversation they want.

In the case of CDMA, what they wind up with is an even thornier problem—a mishmash of half a dozen conversations, each modulated by a different pseudorandom code, all occupying the same band. The signal has to be decoded with the same code, which has been obtained in some mysterious fashion. Plus, in digital systems, voice is vocoded. The sound is not only digitized, but also compressed. As before, someone interested in decompressing it needs to know the compression algorithm used.

In short, eavesdroppers need to build what amounts to the receiving part of a cellular phone base station to have a chance of overhearing a call. Small wonder that none of the system operators or phone manufacturers regard eavesdropping on digital cell phones as a problem.

Ethereal Signatures

The fight against cloning analog handsets has gone a lot better than efforts to combat eavesdropping. Conceived in innocence, early analog phones were almost comically vulnerable to security attacks. For one thing, the signaling between handset and base station takes place in the clear, so anyone with a suitable RF scanner can simply listen-in and learn the phone numbers (called "mobile identity numbers," or MINs) of handsets in the vicinity and the electronic serial numbers (ESNs) that go with them. To program those numbers into another handset is the work of a minute, and behold, another cloned phone is ready for use.

Once the problem manifested itself, service providers began taking steps to protect themselves. Working with the U.S. Secret Service, they persuaded Congress in 1998 to amend the law pertaining to "fraud and related activity in connection with access devices" (Title 18, Section 1029, of the U.S. Code), so as to make it a federal crime to own a scanning receiver or a cell-phone programmer with intent to defraud. That same law also makes it a crime to knowingly, and with intent to defraud, use a counterfeit phone, to traffic in such phones, or to possess 15 or more of them. The law is serious, specifying maximum prison terms of 10 or 15 years (for first-time offenders), depending on the exact nature of the crime.

The service providers also instituted the use of personal identification numbers (PINs) that a user had to key in before a call could be completed. PINs certainly made it tougher for thieves to use stolen phones, but because the PINs were transmitted in the clear, they were not very effective against cloning.

What did help was a technology pioneered by the military for keeping track of enemy troop movements, namely, RF fingerprinting. The technology involves measuring several (unspecified) parameters associated with RF signals and characterizing them (again, in a proprietary manner) to produce a signature unique to the transmitter being studied. Even nominally identical transmitters, manufactured on the same assembly line to the same specifications, have slight differences, which are sufficient (as Corsair named its product) to tell them apart.

Authentication Secrets

With the advent of digital and more advanced analog phones, an even more effective fraud-fighting technology came into use: authentication. A sort of handshaking process, authentication makes use of secret numbers that are stored in the phone and known to the network, but never passed over the air. Every time a call is made, the network sends the handset a random number, which the handset then combines with its secret number using an algorithm designed for the task. The result is another random number that the handset sends back to the network, which has meanwhile performed the same calculations. If the numbers match, the call is completed; if not, it is not.

The algorithm is designed to avalanche very quickly. If the input numbers are off by even a single bit, the resulting number will not even be close to the right answer. Because a different random number is used for each challenge, an eavesdropper would have a hard time figuring out a phone's secret number. This is not to suggest that sophisticated code crackers could not do it (the experts at the NSA would probably consider it a warm-up exercise), but even high-level criminals rarely have access to the required expertise or equipment.

Criminals, by the way, generally clone cell phones not for economic reasons, but rather in the pursuit of anonymity. Eighty-three percent of narcotics dealers arrested in 2001 were found to be in possession of cloned phones, according to testimony from the Drug Enforcement Administration.

Call counting is another technique that can be used instead of (more often, in addition to) authentication. Like authentication, it requires a phone capable of performing its part of the process. With call counting, both the handset and the network track the number of calls made by the handset. Those numbers are compared whenever a call is made. If they do not match or if they disagree by more than a specified amount (generally one call), then the call is not allowed. Obviously, if someone has cloned a phone, then both he or she and the legitimate users will be making calls, so the network will have their combined number, whereas each handset will have only its own.

RF fingerprinting and authentication together have proven extremely effective. Cloning fraud has dropped about 99% over the past four to five years. It has been replaced, however, by another kind of fraud called "identity theft" (as previously discussed), also known as subscription fraud.

Subscriber Fraud

Criminals, like electrons, tend to take the path of least resistance. Make it really hard to steal what they want one way, and they find a different way to get it. In the case of cell phones (or, more accurately, cell-phone service), the defenses in place against cloning have motivated criminals to adopt the various techniques used by credit card thieves, which are all lumped together under the rubric of subscriber fraud.

As with cloning, the industry's first defensive move was to persuade Congress to strengthen the relevant statute (in this case Title 18, Section 1028 of the U.S. Code, "fraud and related activity in connection with identification documents and information"). As the law now stands, it is a federal crime merely to steal someone's identity information with intent to defraud. Previously, the government had to wait until fraud was committed before it could act.

The industry became particularly susceptible to subscriber fraud when it started pursuing new customers through such nontraditional channels as telemarketing and the Internet. Previously, cell-phone service was mostly purchased in face-to-face transactions in company-owned stores, and clerks could do things like check photo IDs to verify a customer's identity. Now companies are finding they will have to get back to the basics if they are to keep subscriber fraud losses at a tolerable level. They are going to have to verify addresses against credit-card databases, for example, but there are legitimate reasons for discrepancies, because people may have just moved or they may maintain multiple residences. Therefore, methods must be developed for screening out bad risks without turning off legitimate customers.

Technology as such is of limited value in this area. One thing computers are being used to do is keep track of subscriber calling patterns—the numbers they tend to call or receive calls from. If a subscriber is terminated for nonpayment of bills and if a "new" subscriber shows up with pretty much the same calling pattern, then an alarm can be raised calling attention to the possibility that this may be the same person, and the company can look more closely at him.

Subsidy Loss

A major problem, especially in Latin America, is cell phones moving sideways through the distribution channels. Cellular handsets are often heavily subsidized by service providers, who supply them to subscribers on condition that the subscribers remain with the company for a specific period, typically a year. What sometimes happens is that the phones wind up being activated on some other carrier's network.

A distributor, for example, who has purchased a batch of subsidized handsets at a low price from one carrier may find that he or she can sell them at a handsome profit to a dealer who is not affiliated with that carrier. In Latin America, that dealer may not even be in the same country as the distributor. As a result, the carrier loses the money it invested in subsidizing the phones.

As with subscriber fraud, the remedy is mostly a matter of running a tighter ship, but some sort of technological fix will also be developed, which can be described as an authentication kind of approach for the activation process. This technology is foreseen as showing up in some second-generation phones and it will be part of any third-generation deployment.

THE NEW ORDER AND STATE MEDICAL ID CARDS

The recent hacking of 9,000 administrative patient files from one of the country's top hospitals underscores the lack of firm, clear, universal standards to ensure the security of online medical records. Although officials are crafting regulations governing electronic patient records for the health care industry, some analysts and industry players are skeptical about how effective these specifications will be.

In an attempt to remedy the situation, the U.S. government is finalizing and releasing the security and privacy portions of the Health Insurance Portability and Accountability Act (HIPAA), which will define interface and security standards and policies. Unless it is derailed by the new administration, both the regulatory commissions that accredit hospitals and the federal agencies that receive complaints will enforce the HIPAA privacy regulations.

Bumpy Road Ahead

The industry still has a long way to go. The privacy provisions are a quagmire. A lot of it is onerous and expensive, and a lot of it hard to interpret (see sidebar, "New Medical Privacy Rules").

NEW MEDICAL PRIVACY RULES

Before President Clinton left office, he announced a sweeping set of federal rules aimed at protecting the privacy of medical records and other personal health information, establishing the potential for penalties to be imposed on executives at health care businesses that breach the new standards.

The regulations, which were prepared by the U.S. Department of Health and Human Services (HHS), are the final version of proposed rules that were issued in 1999 after Congress failed to pass comprehensive medical privacy legislation as required by HIPAA.

Oral, paper-based, and electronic communications are all covered by the measures. That casts a wider net than the original proposal, which applied to electronic records and to paper ones that at some point had existed in electronic form.

Under the regulations, health care providers are prohibited from releasing most information about individual patients without getting their consent in advance. In another change from the proposed rules, HHS indicates doctors and hospitals will be given full discretion in determining what personal health information to include when sending patients' medical records to other providers for treatment purposes.

However, the final rules also tighten the consent requirement, mandating that approval be secured from patients for even routine use and disclosure of health records for purposes such as bill payments. Patients also must be given detailed written information about their privacy rights and any planned use of their personal information.

In addition, HHS is calling on hospitals, health insurers, and health care clearinghouses to establish procedures for protecting the privacy of patients, including

→

the appointment of executives to oversee their internal privacy procedures. Companies are prohibited from accessing health records for employment purposes.

Under HIPAA, civil fines of $100 per violation can be imposed, up to a total of $25,000 per year. Criminal penalties of up to $250,000 and 10 years in prison could also be targeted at individuals who try to profit from the sale of health information. Most health care companies will be given two years to comply with the regulations.

Nothing is more private than medical or psychiatric records, so if the government is to make freedom fully meaningful in the Information Age, when most of the information is on some computer somewhere, then the government has to protect the privacy of individual health records. The regulations were made necessary by the great tides of technological and economic change that have swept through the medical profession over the past few years.

HHS estimates that complying with the HIPAA rules will cost the health care industry $40.9 billion. In the long run, government officials claim, the regulations will help achieve savings of almost $60 billion over the next 10 years, as a result of related rules that eliminate paperwork by issuing standards for electronic communication of health insurance claims.

The government is expected to receive a lot of backlash regarding the inclusion of paper and oral communications in the new rules. Originally, HIPAA was intended to apply solely to electronic communications. It could be impossible to monitor written and oral messages.

One of the problems is that HIPAA is supposed to offer specifications to cover all privacy implementations, from one-doctor offices to giant health care organizations. It's too strict in many respects and too loose in others to offer adequate regulations across the board.

Lessons to Learn

However, there is a whole range of institutions that must be educated on any guidelines to be implemented, including third-party companies that offer electronic patient-record hosting or storage [4]. With start-ups, patients face the risk that companies that store their records online will go out of business. A bankrupt company could sell its data to a company with a different privacy policy.

Despite the obstacles, online medical records will eventually gain more general acceptance [5]. The biggest resistance is fear. Once fear is behind the patients and the companies that store their records, online medical records can really take off.

BIG BROTHER IS HERE AND IS STAYING

Workplace surveillance was the leading privacy concern in 2004, according to an analysis recently released by the Privacy Foundation, a Denver-based nonprofit group that performs research and educates the public on privacy issues. In 2004, millions of Americans were watched at work, as employers became increasingly concerned about employee productivity and their use of the Internet. Three-fourths of major U.S. companies now perform some type of in-house electronic surveillance according to the American Management Association, and 32% of all companies surveyed now monitor email.

The Big Brother tactic has led to some people losing their jobs. Dow Chemical fired 68 employees and disciplined 679 others in 2004 for allegedly storing and sending sexual or violent images on the company's computers. Xerox, the New York Times Co., and the CIA were others that fired or disciplined employees because of alleged bad behavior.

Employers may be rightly concerned about security and productivity issues, or legal liability arising from emailed sexual banter. But pervasive or spot-check surveillance conducted through keystroke monitoring software, reviewing voice-mail messages, and using mini video cameras will undoubtedly affect morale and labor law, as well as employee recruitment and retention practices.

In the future, the Privacy Foundation predicts that employers, especially so-called new economy companies, may offer "spy-free" workplaces as a fringe benefit—but only as a fringe benefit. Big Brother is here and staying, and, it's only going to get worse.

Big Brother Is Watching and Listening

"How the United States Spies on You," read the afternoon headline in *Le Monde* [6], enough, certainly, to jolt Parisians on their commute home. Across Europe recently, politicians and the press were in full cry over a vast Anglo-American electronic surveillance system named Echelon. The system scans billions of private emails, faxes, and telephone conversations each hour, according to a report debated by the European Union Parliament. Echelon, said Parliament President Nicole Fontaine, is "a violation of the fundamental rights" of European Union citizens.

The most incendiary charge is that Echelon represents economic espionage nonpareil, helping the United States and its English-speaking allies steal trade (and jobs) from non-Anglos. Charges cited are mostly old, well-known cases: In 1994, U.S. intelligence discovered that French companies were offering bribes to Saudi Arabia and Brazil for multibillion-dollar contracts. Washington complained, and U.S. firms got the deals.

U.S. officials insisted last week that American intelligence does not steal trade secrets for U.S. firms. Even if it tried, the NSA, which oversees Echelon, is drowning in data thanks to the global communications revolution. In some ways, people's communications have never been safer from becoming intelligence, and France is certainly not a slouch in the industrial espionage arena.

Although it has the added spice of Internet-age privacy concerns, the Echelon flap revealed anew how Europe and the United States are increasingly at odds over matters from defense cooperation to genetically engineered "frankenfoods." Just a few days earlier, a French intelligence report suggested the NSA helped create Microsoft to eavesdrop around the world. The loser this time may be the United Kingdom, whose special intelligence-sharing accord with Washington looks to some like disloyalty to the EU.

BioFusion

Buck Rogers, meet John Norseen. Like the comic-strip hero, a 20th-century man stuck in the 25th century, Norseen feels he's not quite in the right time: his brain-research ideas are simply too futuristic, and he admits his current obsession seems to have been lifted from a Rogers saga. The Lockheed Martin neuroengineer hopes to turn the "electrohypnomentalophone," a mind-reading machine invented by one of Buck's buddies, from science fiction into science fact.

Norseen's interest in the brain stems from a Soviet book he read in the mid-1980s, claiming that research on the mind would revolutionize the military and society at large. The former Navy pilot coined the term *bioFusion* to cover his plans to map and manipulate gray matter, leading (he hopes) to advances in medicine, national security, and entertainment. He does not do the research but sees himself as the integrator of discoveries that will make bioFusion a reality and the ultimate IW weapon for Big Brother.

BioFusion would be able to convert thoughts into computer commands, predicts Norseen, by deciphering the brain's electrical activity. Electromagnetic pulses would trigger the release of the brain's own neurotransmitters to fight off disease, enhance learning, or alter the mind's visual images, creating what Norseen has dubbed "synthetic reality."

The key is finding "brain prints." Think of your hand touching a mirror. It leaves a fingerprint. BioFusion would reveal the fingerprints of the brain by using mathematical models. Just like you can find one person in a million through fingerprints, you can find one thought in a million.

It sounds crazy, but Uncle Sam is listening and watching. NASA, DARPA, and the Army's National Ground Intelligence Center have all awarded small basic research contracts to Norseen, who works for Lockheed Martin's intelligent systems division. Norseen is waiting to hear if the second stage of these contracts (portions of them classified) comes through.

Norseen's theories are grounded in current science. Mapping human brain functions is now routine. By viewing a brain scan recorded by a magnetic resonance imaging (MRI) machine, scientists can tell what the person was doing at the time of the recording, for example, reading or writing. Emotions from love to hate can be recognized from the brain's electrical activity.

Applying Neuroscience Research to Antiterrorism

Norseen has submitted a research and development plan to the Pentagon, at its request, to identify a terrorist's mental profile. A miniaturized brain-mapping device inside an airport metal detector would screen passengers' brain patterns against a dictionary of brain prints. Norseen predicts profiling by brain print will be in place by 2009.

A pilot could fly a plane by merely thinking, indicates Norseen. Scientists have already linked mind and machine by implanting electrodes into a paralyzed man's brain; he can control a computer's cursor with his mind. Norseen would like to draw on Russian brain-mimicking software and American brain-mapping breakthroughs to allow that communication to take place in a less invasive way. A modified helmet could record a pilot's brain waves. When you say "right 090 degrees," the computer would see that electrical pattern in the brain and turn the plane 090 degrees. If the pilot misheard instructions to turn 090 degrees and was thinking "080 degrees," the helmet would detect the error, then inject the right number via electromagnetic waves.

Finally, if this research pans out, you can begin to manipulate what someone is thinking even before they know it. Norseen feels he is "agnostic" on the moral ramifications, that he's not a mad scientist—just a dedicated one. The ethics don't concern him, but they should concern someone.

SUMMARY

This chapter has considered the application of civilian information operations (CIOs) to the conventional warfare environment. Although the array of CIO tools and techniques has been presented as discrete elements in a schematic diagram, the CIO environment is complex, multidimensional, interactive, and still developing. Accordingly, the introduction of a CIO capability into an existing military force requires careful consideration and adherence to a series of principles espoused within this chapter. These principles are defined within a framework of concepts including information assurance, information superiority, and information dominance.

This framework can be applied to both the introduction of a CIO capability and the application of CIO's in information warfare.

CIOs will change the nature of future wars and will eventually evolve into a separate paradigm of warfare—IW. However, CIOs can be applied to today's conventional environment, and it is within this context that more urgent attention from military planners is required. CIOs offer both a support capability to existing arms of the military and an additional dimension to conventional warfare. They may be used to strike enemy systems, control the overall information environment, deter enemy aggression, or support either themselves or other military strategies. Regardless of which tasks they are employed for, CIOs offer a significant addition to the conventional inventory and should be developed as a matter of priority as an essential joint force operational capability in dealing with the civilian casualties of IW as follows.

Conclusions

- Information warfare (IW) is the latest development in a long list of revolutions in military affairs based on new technology (other examples include the introduction of airplanes, the atom bomb, and long-range missiles).
- IW is defined as an attack on information systems for military advantage using tactics of destruction, denial, exploitation, or deception.
- Information systems are so critical to military operations that it is often more effective to attack an opponent's information systems than to concentrate on destroying its military forces directly.
- In the civilian context, the U.S. economic, social, and political structures are increasingly dependent on complex and extensive systems for financial transactions, telecommunications, electric power, energy distribution, and transportation. Because these systems rely on each other, a serious disruption in any one system will cascade quickly through the other systems, potentially causing a national security crisis. Under these circumstances, the ability of the government to respond will be interrupted and severely constrained.
- In addition to outages caused by natural disasters and accidents, these systems present a tempting target for IW attack to those contemplating an action against U.S. interests.
- IW provides a new context for the application of ethical theories.
- The ethical questions about IW are not meant to be a complete set of ethical questions, but rather a subjective assessment of what are the ethical questions derived from the most important issues exposed by IW.
- New unforeseen ethical questions will inevitably arise from IW in the near future.
- It is hoped that this research will begin a dialog on the issues and lay a framework for more substantive work by ethicists.

- IW and its complement (protection from IW) require important new research efforts from both the technology and ethics research communities.
- The threat of IW raises the following ethical challenges: (1) What constitutes an act of war in the Information Age? (2) What are the ethical implications of the blurring distinction between acts of war, acts of espionage, and acts of terrorism? (3) Can IW be considered nonlethal? (4) Is it ethical to set expectations for a "bloodless war" based on IW? (5) Is it ethically correct to respond to IW tactics with IW tactics? (6) Can protection from IW take place in the United States, given our democratic freedoms?

An Agenda for Action

Three policy questions dominate the issue of critical infrastructure protection for civilian casualties of IW: how limited should the government's role be, what is adequate infrastructure security and how will appropriate standards be determined, and what data does the government need from business and why? None seems fundamentally settled, if only because policy continues to develop. There are more questions than answers. Nonetheless, a few basic principles are emerging that should guide infrastructure protection efforts.

The U.S. government needs to set an agenda for action that goes beyond the work already done in preparation for civilian casualties of IW. Action steps should include, but not be limited to the 10 areas as shown in Table F19.1 of Appendix F.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Information warfare (IW) is the latest development in a short list of revolutions in military affairs based on new technology (other examples include the introduction of airplanes, the atom bomb, and long-range missiles).
2. True or False? Information systems are so critical to military operations that it is often less effective to attack an opponent's information systems than to concentrate on destroying its military forces directly.
3. True or False? IW is defined as an attack on information systems for military disadvantage using tactics of destruction, denial, exploitation, or deception.

4. True or False? Old unforeseen ethical questions will inevitably arise from IW in the near future.
5. True or False? IW provides an old context for the application of ethical theories.

Multiple Choice

1. The following are critical national infrastructures as listed by the executive order, except:
   A. Electric power system
   B. Gas and oil storage and transportation
   C. Web site
   D. Banking and finance
   E. Transportation
2. For a strategy of deterrence to work the following must hold, except:
   A. The incident must not be well defined.
   B. The identity of the perpetrator must be unambiguous.
   C. The will and ability to carry out a deterrence strike must be believed.
   D. The perpetrator must have something of value at stake.
   E. The deterrence strike must be controllable.
3. In what has been called the "complex-system issue," the following are axioms, except:
   A. Complex systems fail in unpredictable ways from causes that seem to be minor and, often, obvious flaws in retrospect.
   B. Complex systems pass in unpredictable ways from causes that seem to be minor and, often, obvious flaws in retrospect.
   C. The failure of a complex system may be exceptionally difficult to discover and repair.
   D. Complex systems fail at inopportune moments—usually during demanding system use when the consequences of failure are highest.
4. The following requirements of *jus ad bellum* were developed by Thomas Aquinas in the 13th century, except:
   A. The resort to force must have a just cause.
   B. It must be authorized by a competent authority.
   C. It is expected to produce a preponderance of evil over good.
   D. It must have a reasonable chance of success.
   E. It must be a last resort.

5. By changing perspectives from defense to offense, the following are in the U.S. arsenal to wage IW against an adversary, except:
   A. Offensive software (viruses, worms, trojan horses)
   B. Sniffing or "wiretapping" software (enabling the capture of an adversary's communications)
   C. Chipping (malicious software embedded in systems by manufacturer)
   D. Directed non-energy weapons (designed to destroy electronics, not humans and buildings)
   E. Psychological operations (sophisticated and covert propaganda techniques)

Exercise

A global supplier of integrated circuits for personal and networked computers also produces microprocessors, flash memory devices, and silicon-based solutions for communications and networking applications, at manufacturing facilities in the United States, Europe, Japan, and Asia. The company has been conducting internal investigations since the late 1990s, but they needed to ensure that they had the proper processes in place to meet federal requirements regarding rules of evidence. How was the computer forensics specialist team (CFST) able to go about conducting the company's investigation?

HANDS-ON PROJECTS

With 650 attorneys in 9 U.S. offices and a global reach throughout Europe, Asia, and Latin America, a large law firm serves many of the world's largest and best-known businesses, nonprofit organizations, and individuals. Founded in 1906, the firm is a leader in innovative legal services—overseeing the functionality and maintenance of approximately 1,800 machines on a daily basis. The use of a CFS at the firm falls into several different categories surrounding internal compliance and policy enforcement: inappropriate usage, where users might be violating internal corporate policy and visiting inappropriate outside sites; intentional misuse, where users have done something they know is inappropriate and there is a need to find out where the action originated; and, the search for specific information. These areas may also overlap during an investigation. For intentional misuse, the firm used a CFS to reach out and find where an action originated to help them build a case to refer to human resources. How would a CFS go about conducting an investigation under these circumstances?

Case Project

An incident was discovered by a global pharmaceutical and medical manufacturing company that caused major concerns. Their email filtering tool had identified dialog from a senior manager's email account that contained inappropriate statements. This manager was a 20-year veteran who had an impeccable employee record, and prior to this incident the employee's behavior had never been in question. Further investigation was required to confirm or deny the alleged behavior. It was very important to be able to respond quickly to resolve the potential situation, and to be discreet, in order to protect the manager's privacy and good reputation. How did the CFS go about conducting the investigation?

Optional Team Case Project

A CFS was hired by a client to investigate the theft of trade secrets by a former employee. A product manufacturer (client) alleged that a former employee removed files containing corporate secrets from their computer systems and then used these secrets as the basis for establishing a new company, making a competitive product line, and marketing to the client's customer base. Litigation had been ongoing for two years, allowing the opposition to continue their business operations and begin to target the suppliers and vendors of the client, resulting in significant lost revenue. How was the CFS able to go about conducting the investigation?

REFERENCES

[1] Vacca, John R., *Satellite Encryption*, Academic Press, New York, 1999.

[2] Vacca, John R., *Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan*, McGraw-Hill, New York, 2001.

[3] Vacca, John R., *Identity Theft*, Prentice Hall, New York, 2002.

[4] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

[5] Vacca, John R., *Public Key Infrastructure: Building Trusted Applications and Web Services,* Auerbach Publications, Boca Raton, FL, 2004.

[6] Cypel, Sylvain, "How the United States Spies on You," *Le Monde*, March 5, 2002.

This page intentionally left blank

Part V

Advanced Computer Forensics Systems and Future Directions

The fifth part of this book discusses advanced computer forensics, with a summary, conclusions, and recommendations.

This page intentionally left blank

20 Advanced Computer Forensics

The rise of the so-called information economy, borne along by proliferating computers, sprawling telecommunications, and the Internet, has radically transformed how people do business, govern, entertain themselves, and converse with friends and family. Private documents that in the past would have been committed to paper and hand-delivered or stowed under lock and key are now routinely created, sent, and stored electronically.

The very things that allow such speed and ease of communication have also made it far more difficult to ensure one's privacy [1]. In an electronic age, an interloper can intercept and alter messages far more easily now than when face-to-face exchanges were the norm. Mounting concern over the new threats to privacy and security has led to widespread adoption of cryptography. Once the purview of professional spies, strong encryption is now available worldwide to any amateur with a PC and inexpensive, off-the-shelf software.

Over the past two decades, individuals and businesses alike have embraced the technology, using it for everything from sending email and storing medical records and legal contracts to conducting online transactions. Cryptographic algorithms are written into all the most popular World Wide Web browsers and can be readily incorporated into most email programs.

If ordinary individuals can now encrypt a message in all but unbreakable form, then so can criminals, terrorists, and other troublemakers. That prospect has governments on edge. In the past, armed (or not) with a court warrant, police could readily get at hidden documents by, for example, forcing a safe, but physical force is of no use in decoding computer-encrypted data.

This turn of events has led many governments worldwide to view the technology as a grave threat to social order and to seek to control its spread. Repressive regimes fear that dissident groups will use encryption to promote their subversive ideas. Democratic governments, too, fret over the possibility that encryption will be used to further the activities of drug dealers, militant dissenters, and assorted enemies of the state. Indeed, the U.S. government once categorized encryption technology as a controlled munition, on a par with nuclear weapons, and until very recently it banned the export of the most advanced encryption products.

State controls have met with fierce protests, pitting governments against an unlikely confederacy of privacy rights advocates, cryptography experts, and corporations with a financial stake in promoting encryption's use. The ensuing battle over encryption has taken on several dimensions—technical, legal, ethical, and social. At times, the arguments have assumed the same rigidity and polarization as certain religious debates.

With the rise of hard-to-crack encryption, sensitive data is easier to protect—and criminal activity tougher to monitor. The following section will review the advanced encryption techniques now available worldwide and discuss the legal campaigns that governments have mounted in response, including the changes recently proposed to U.S. export laws.

ADVANCED ENCRYPTION: THE NEED TO CONCEAL

On German television several years ago, a stunned audience looked on as an unsuspecting Web surfer had his computer scanned while he was visiting a site. The site operators determined that a particular online banking program was installed on his computer, and they remotely modified a file in it so that the next time the user connected to his bank online, he also directed his bank (unbeknownst to him) to send a payment to the owners of that Web site.

The vulnerability of computer data affects everyone. Whenever a computer is connected to a network, be that a corporate intranet or the Internet, unless proper precautions are taken, the data residing in the machine can be accessed and otherwise modified by another knowledgeable user. Even computer data that the user may believe to be deleted or overwritten can be retrieved. Courts now routinely subpoena individuals' and companies' magnetic media as evidence; forensic experts can reconstruct data files that have been erased. In these cases, possession is not nine-tenths of the law. The best way to protect electronic data is to encrypt it.

The purpose of encryption is to render a document unreadable by all except those authorized to read it. The content of the original document, referred to by cryptographers as "plaintext," is scrambled using an algorithm and a variable, or key. The key is a randomly selected string of numbers; generally speaking, the longer the string, the stronger the security.

Provably unbreakable encryption has been around since the dawn of recorded history, and although computers have made encryption more accessible, they are certainly not a requirement. One precomputer method is the conceptually simple, yet very strong, encryption scheme known as the one-time pad, developed in 1926 by Gilbert S. Vernam (see sidebar, "Computer-Free Encryption").

NOTE

The term "unbreakable encryption" is somewhat misleading. In many cases, the plaintext has a limited lifespan, and so the protection afforded by encryption need not last forever. Tactical data, for example, often requires encryption that takes only slightly longer to break than the useful life of that data. This is often forgotten in debates about the relative strengths of encryption methods.

COMPUTER-FREE ENCRYPTION

The durable encrypting scheme known as the one-time pad gets its name from the use of a key once and once only for just one message. It works like this:

Toni, the sender of a sensitive message wakes up one morning and starts shouting out two-digit numbers at random: 56, 34, 01, 92, 27, 11, and so on. These numbers become the key. Toni then assigns a sequential number to each letter of the alphabet: A = 01, B = 02, C = 03, D = 04, E = 05, and so on.

Next, she encodes the plaintext word "hello," which, in accordance with the preceding sequential numbering of the letters, corresponds to the sequence 08, 05, 12, 12, 15. She then does a simple modulo-10 addition with no carry, using the key she generated in the preceding. In other words,

H E L L O

08 05 12 12 15

+ 56 34 01 92 27

____

= 54 39 13 04 32

This last sequence (54, 39, 13, 04, 32) is the ciphertext, which gets sent to Wolfgang, the intended recipient. Note that the same plaintext letters do not necessarily get encrypted into the same ciphertext symbols (the letter L is both 13 and 04 in this case).

→

Wolfgang has an exact copy of the key (56, 34, and so on). To decode Toni's message, he does the reverse operation, again with no carry:

54 39 13 04 32

_ 56 34 01 92 27

= 08 05 12 12 15

= H E L L O

Generating long keys by "shouting out" long strings of numbers can be impractical, so in modern applications of the one-time pad, computers are often assigned to create the keys. The result is not truly random: computers' pseudorandom number generators use only 16 (or, in some cases, 32) bits to store their values. The entire space of such values can be searched within a week or so. One remedy is to tweak the pseudorandom number generator by applying an external physical process to generate noise—maybe a sufficiently amplified semiconductor junction of 1/f noise—but that further requires removing the influence of predictable external influences, such as 50–60-Hz noise.

A self-evident shortcoming of the one-time pad is that the key is at least as long as the plaintext being encrypted. To escape cryptanalytic attacks involving statistical analyses, the key must be used only once. A more serious shortcoming is that the same key is used to both encrypt and decrypt. The sender and the recipient, therefore, need a totally secure opportunity to exchange the key, which is hard to come by when the two are far apart.

An amusing feature of the one-time pad is that a fake key can be created that will "decode" the encrypted document into something quite innocent—an excerpt from the Bible, say, or the Bill of Rights. Alternatively, a fake key could be designed to yield a plausible-looking, but still false, document, thereby fooling people into believing they have cracked the code [2].

Symmetric Encryption

Vernam's one-time pad is an example of symmetric encryption, in which the same key is used to both encode and decode a message. Many of the encryption schemes available today are also symmetric, most notably the Data Encryption Standard, or DES (see sidebar, "A Menu of Symmetric Encryption Algorithms").

A MENU OF SYMMETRIC ENCRYPTION ALGORITHMS

In symmetric encryption, the same key is used to encrypt and decrypt a message. Here are the most popular.

The Data Encryption Standard

DES was developed in the 1970s and is still used worldwide, although it has been replaced by the Advanced Encryption Standard (AES).

Triple DES

Encrypting the already DES-encrypted output with a different output with a different key provides no measurable security, but adding a third round of DES encryption yields a highly secure, albeit slower, algorithm. Most purportedly triple-DES implementations, however, use only two keys: key 1 for the first round of encryption, key 2 for the second round, and key 1 again for the third round.

The International Data Encryption Algorithm

The international data encryption algorithm (IDEA) uses a 128-bit key developed by ETH Zurich, in Switzerland. Its U.S. and European patents are held by Ascom Systec Ltd. of Bern, Switzerland, but noncommercial use is free. IDEA is viewed as a good algorithm for all except the best-funded attacks. It is used in Pretty Good Privacy (PGP) and Speak Freely (a program that allows an encrypted digitized voice to be sent over the Internet).

Blowfish

Blowfish is a 64-bit block code with key lengths of 32 to 448 bits. Developed in 1993 by Bruce Schneier of Counterpane Internet Security Inc., San Jose, California, it is used in over 100 products and is viewed as one of the best available algorithms.

Twofish

Twofish, also developed by Schneier, is reputedly very strong, and, as one of five candidates for AES, is now being extensively reviewed by cryptanalysts.

→

RC4

RC4 is a stream cipher of unknown security, designed by Ronald Rivest for RSA Security Inc., Bedford, Massachusetts. It adds the output of a pseudorandom number generator bit by bit to the sequential bits of the digitized plaintext [2].

Developed in the 1970s, DES is still popular, especially in the banking industry. It is a block cipher, meaning that it encodes text in fixed-bit blocks using a key whose length is also fixed in length. The alternative, known as stream ciphers, encode the stream of data sequentially without segmenting it into blocks.

After nearly three decades of use, DES is headed for the garbage can. Currently, AES has already replaced DES in many organizations worldwide. In all likelihood, AES will become nearly as ubiquitous as its predecessor. Unlike DES, however, it will be competing with other algorithms—algorithms that will not suffer from any suspicion that the U.S. government has a back door into the code.

For some encryption algorithms, a plaintext that is repetitive will result in a repetitive ciphertext. This is clearly undesirable because the encrypted output betrays important information about the plaintext. One solution is to encrypt the ciphertext block and add it bit by bit to the sequential bits of the previously encrypted plaintext.

Another problem with symmetric key encryption is that it requires that the sender and recipient of a message have a secure means for exchanging the encryption key. This is clearly difficult when the two parties are far apart, and the problem is compounded every time the keys are updated. Repeated use of the same key creates its own security weakness.

Public Key Encryption

An ingenious scheme that avoids many of the problems of symmetric encryption was proposed in 1976 by Stanford professor Martin Hellman and his graduate student Whitfield Diffie. Their public key encryption scheme, first described in *IEEE Transactions on Information Theory*, allows the recipient to verify that the sender is who he or she appears to be and that the message has not been tampered with.

The method works like this: Bob and Alice have a copy of openly available software that implements the public-key algorithm. Each directs his or her copy of the software to create a key, or rather, a pair of keys. A file encrypted with one key of a pair can only be decrypted with the other key of that same pair, one key cannot be mathematically inferred from the other key in the pair.

Bob makes known (by email, by posting to a Web site, or however else he chooses) one of the keys of his pair; this becomes his public key. Alice does the same. Each retains under tight control the other key in the pair, which is now his or her private key.

If Bob wants to encrypt a message that only Alice can read, he uses Alice's public key (which is available to anyone); that message can only be decoded by Alice's private key (Figure 20.1) [2]. The reciprocal process (sending an encrypted message from Alice to Bob) is clear. In effect, Bob and Alice can now exchange encrypted

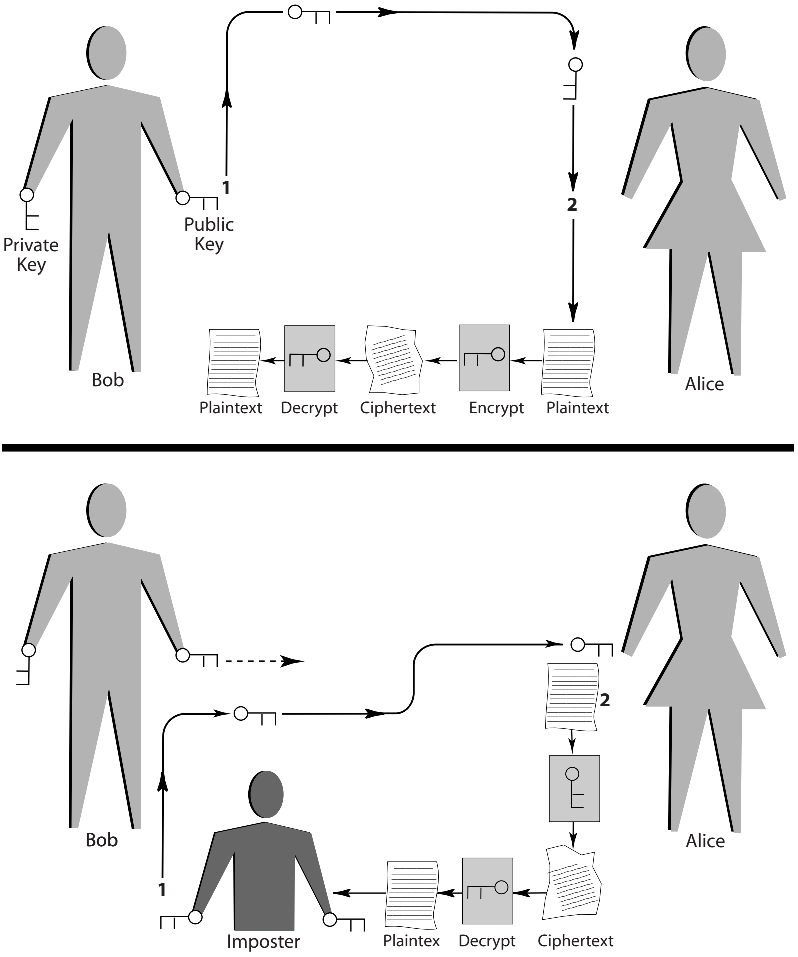


FIGURE 20.1 In public-key encryption [top], Alice encrypts a message using Bob's public key, and Bob decrypts it using his private key. This scheme allows encrypted files to be sent in the absence of a secure means to exchange keys, a major improvement over symmetric encryption. It's still possible, though, for Alice to receive a public key (or a conventional symmetric key) that ostensibly came from Bob, but that, in fact, belongs to a third party claiming to be Bob—the so-called man-in-the-middle attack (bottom).

files in the absence of a secure means to exchange keys, a major advantage over symmetric encryption.

Sender authentication verifies that the sender is who he or she appears to be. Suppose Bob sends a message to the world after encrypting it with his private key. The world uses Bob's public key to decrypt that message, thereby validating that it could only have come from Bob.

Message authentication, the validation that the message received is an unaltered copy of the message sent, is also easy: Before encrypting an outgoing message, Bob performs a cryptographic hash function on it, which amounts to an elaborate version of a checksum. The hash function compresses the bits of the plaintext message into a fixed-size digest, or hash value, of 128 or more bits. It is extremely difficult to alter the plaintext message without altering the hash value (Figure 20.2).

The widely used hash function MD5, developed by Rivest in 1991, hashes a file of arbitrary length into a 128-bit value. Another common hash function is SHA (Secure Hash Algorithm), published by the U.S. government in 1995, which hashes a file into a longer, 160-bit value.

Public-key encryption has been a part of every Web browser for the past few years. It is used, for example, when sending credit-card information to an online vendor or when sending email using the standard S/MIME protocol and a security certificate, which can either be obtained from online commercial vendors or created locally using special software.

One drawback of public key encryption is that it is more computationally intensive than symmetric encryption. To cut back on the computing, almost all

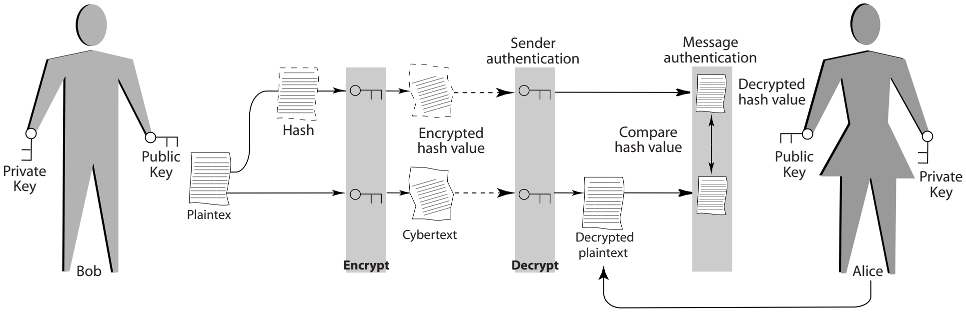


FIGURE 20.2 Public key encryption allows Alice to verify that a message from Bob actually came from him and that it is unaltered from the original. Here's how: Bob encrypts the hash value with his private key, encrypts the plaintext with Alice's (green) public key, and sends both to her. Alice then decodes the received ciphertext using her own (orange) private key, decodes the hash value using Bob's public key, thereby confirming the sender's authenticity, and compares the decrypted hash value with one that she calculates locally on the just decrypted plaintext, thereby confirming the message's integrity.

implementations call on the symmetric approach to encrypt the plaintext and then use public key encryption to encode the local key. The differently encrypted plaintext and key are then both sent to the recipient.

In terms of resistance to brute force cryptanalysis (the exhaustive search of all possible decryption keys) a good 128-bit symmetric encryption algorithm is about as strong as a 2,304-bit public key algorithm. Realistically, though, the public key should be even longer than that, because the same public and private key pair is used to protect all messages to the same recipient. In other words, although a broken symmetric key typically compromises only a single message, a broken public key pair compromises all messages to a given recipient. To be sure, cracking an encryption key is just one way to get at sensitive data (see sidebar, "Human and Hardware Frailties").

HUMAN AND HARDWARE FRAILTIES

The encryption of material to withstand a brute force attack still leaves many avenues open to invasion. Often, the real weaknesses in security lie in the human tendency to cut corners. It is all too tempting to use easy-to-remember passwords or keep unencrypted copies of sensitive documents on one's computer, intentionally or otherwise. Windows-based computers and many software products, in their quest to be user-friendly, often leave extensive electronic trails across the hard drive. These trails include not only copies of unencrypted files that the user deleted but also passwords and keys typed.

Furthermore, unless each file is encrypted using a different key or a different encryption method, an attacker who can somehow read one encrypted file from or to a given person can probably also read many other encrypted files from or to that person.

Cryptanalysts have also been known to exploit the hardware on which the encryption algorithm is used. In 1995, the so-called timing attack became popular. It allowed someone with access to the hardware to draw useful inferences from the precise time it took to encrypt a document using a particular type of algorithm. Public key encryption algorithms such as RSA and Diffie-Hellman are open to such attacks. Other exploitable hardware phenomena include power consumption and RF radiation. It is also possible to assess the electronic paper trail left behind when the hardware is made to fail in the course of an encryption or decryption.

Most of today's commercial email programs, Web browsers, and other Internet applications include some encryption functions. Unfortunately, these schemes are often implemented as an afterthought by engineers who may be very competent in their respective fields but have minimal experience in cryptography.

→

Just like a decent forgery, bad encryption can look like good encryption on the surface. In general, however, "proprietary," "secret," or "revolutionary" schemes that have not withstood the scrutiny of cryptanalysts over time are to be avoided.

One easy test is to attempt to decrypt a file with a different key from the one used for encryption. If the software proudly informs the user that this is the wrong key, that encryption method should be discarded. It means that the encryption key has been stored in some form along with the encrypted file. The cryptanalyst would merely have to keep trying different keys until the software identified the correct one. This is only one of many weaknesses. Given the preceding, the odds favor the person attacking an encrypted file, unless the person being attacked is very knowledgeable in the ways of information security [2].

Public key encryption is also a victim of the uncertainty besetting any cryptographic scheme when the two communicating parties lack a secure channel by which to confirm the other's identity (Figure 20.1). There is, as yet, no technical fix to this problem.

One of the most commonly used public key algorithms is the 24-year-old RSA, named for its creators, Ronald Rivest, Adi Shamir, and Leonard Adleman of the Massachusetts Institute of Technology, Cambridge. Its security derives from the difficulty of factoring large prime integers. At present, a key length of at least 1,024 bits is generally held secure enough. However, RSA may be somewhat vulnerable to "chosen plaintext attacks," attacks in which the cryptanalyst already possesses a plaintext file and the corresponding RSA-encrypted ciphertext.

The Diffie-Hellman public key algorithm is used mostly for exchanging keys. Its security rests on the difficulty of computing discrete logarithms in a finite field generated by a large prime number, which is regarded as even harder than factoring large numbers into their prime-number components. The algorithm is generally viewed as secure if long enough keys and proper key generators are used.

By far the most popular public key encryption scheme is PGP (pretty good privacy). PGP was created in 1991 by a programmer and activist named Philip Zimmermann as a means of protecting email. After one of his colleagues posted PGP on the Internet, the Department of Justice launched an investigation of Zimmermann for possible violation of U.S. laws governing export of encryption products. The case against him was eventually dropped in 1996, after which Zimmermann started a company to market PGP. It has since become a mainstream commercial product, sold by Network Associates Inc., of Santa Clara, California, although freeware versions continue to be available from the Internet.

Crackdown on Cryptography

What happened to Zimmermann is just one small skirmish in the much wider campaign waged by governments worldwide against cryptography. At issue is whether, and to what extent, persons and organizations should have the ability to encrypt information that the state cannot decipher.

Private citizens have legitimate reasons to preserve confidentiality: to protect trade secrets, to prevent legal or medical records from falling into strangers' hands, and to voice dissenting political or religious opinions without retribution. The international group Human Rights Watch, for example, regularly encrypts eye-witness reports of serious abuse, gathered in parts of the globe where the victims may be subject to further reprisals.

From a government's perspective, however, encryption is a double-edged sword: it has honorable purposes, true, but it can also be used to conceal out-and-out criminality. In an effort to keep encryption from gaining ground, many countries have passed laws criminalizing its import, export, and use.

NOTE

To be sure, exactly what constitutes a crime is not always clear; governments have been known to capitalize on the use of the term "criminal" and apply it to conduct they dislike or consider threatening.

The proliferation of encryption has coincided with the explosive growth of the Internet. Nowadays, the man in the street can reach an instant global audience of millions, bypassing the chain of command that rules almost any institution, be that the military, a religious group, or a corporation. In essence, the simultaneous spread of encryption and the Internet has amounted to a transfer of power to the individual.

This turn of events has been viewed differently by different states. An interesting case is the People's Republic of China. There, the outlawed religious sect Falun Dafa has used the Web to great effect to spread its ideology and recruit new members. Repeated attempts by the authorities to shut down the group have largely failed. Recently, the government began requiring any company doing business in China to disclose the types of Internet encryption software it uses, as well as the names of employees who use it. It further banned the sale of foreign-designed encryption products. Overseeing the regulations is a newly established body, the State Encryption Management Commission, which is believed to be staffed by China's secret police.

China's unwavering opposition to encryption suggests a more fundamental reason why a government (any government) would want to control the technology: to preserve the ability to exercise censorship. Even enlightened and democratic regimes have topics that are taboo, and when any and all information being exchanged by private citizens can be monitored, it has a chilling effect on dissenting opinions. Conversely, when citizens can communicate freely and privately using encryption, censorship becomes unenforceable. Few sovereign states can accept this loss of control. It's like having two rude guests at one's dinner table who keep whispering in each other's ears.

Encryption, though, is good for business, and that factor is largely responsible for the gradual relaxing in the U.S. government's stance on encryption. Until 1996, strong encryption technology was listed as a munition, and until just recently, it fell under the same export restrictions as advanced weaponry. Under concerted pressure from the U.S. business community, which claimed that such controls were reducing sales and choking the growth of electronic commerce, the government came out with a revised policy recently that lifts many of the bureaucratic burdens from companies wanting to export encryption. Even so, every encryption product must still undergo a one-time review by the U.S. Commerce Department's Bureau of Export Administration before it can be exported; sales to the so-called terrorist five (Cuba, Iran, North Korea, Sudan, and Syria) are still excluded. The new stipulation has some cynics wondering if only products with an identifiable weakness will receive an export license.

What's more (although encryption proponents have largely welcomed the relaxation of export rules), another concern has been raised: the same legislation would grant law enforcement new powers, such as the right to present a plaintext in court without disclosing how it was obtained from a suspect's encrypted files. Here the potential for abuse is obvious.

Other Legal Responses

The United States is not alone in backing away from strict encryption bans. What started as a global campaign to limit encryption has splintered into various approaches, with some governments now even encouraging encryption among their citizens as a precaution against snooping by other governments.

Generally speaking, laws pertaining to encryption are quite convoluted and rife with exceptions and qualifications. In Sweden, for instance, encryption importation and use are allowed, and so is its export, except to certain countries; authorities may search someone's premises for a decryption key but may not compel the person to assist in the investigation by, for example, handing over the key to the authorities.

The first international attempt to control encryption was made by the 17-country Coordinating Committee for Multilateral Strategic Export Controls (COCOM), which came together in 1991 to restrict the export of items and data deemed "dangerous" if acquired by particular countries. COCOM members, with the notable exception of the United States, permitted the export of mass-market and public domain cryptography and restricted export of strong encryption to select countries only. One such item was Global System for Mobile Communications (GSM) cellular telephony [3], which has two grades of encryption. Under COCOM, only the lower-grade version could be sent to the restricted countries.

Both grades of encryption have since been broken.

In March 1994, COCOM was dissolved, to be replaced the following year by the multilateral Wassenaar Arrangement, which has now been joined by (at last count) 66 countries. Under the nonbinding agreement, countries agreed to restrict the export of mass-market software with keys longer than 64 bits.

The arrangement, administered through a small office in Vienna, Austria, is not a treaty, and thus not subject to mandatory review by any country's legislature.

Do such encryption bans work? In a word, no. For one thing, the penalty for using encryption is likely to be far less than the damage caused by disclosing whatever was deemed sensitive enough to warrant encryption. What's more, sophisticated techniques for hiding data, unencrypted or not, are now readily available and extremely hard to detect, so that prosecution of cryptography-ban violations is all but impossible. Who can prove that an innocuous-sounding email message reporting "The temperature in the garage was 86 degrees" really means "Meet me behind Joe's garage on August 6"? out of tens of millions of digitized images posted to a Usenet electronic bulletin board, who can detect the one image in particular, perhaps of an antique car, that contains a secret message intended for a specific person, who along with millions of unsuspecting others will download that image to his or her computer?

The very existence of the Internet has made it easy to circumvent bans. In most, though not all, countries, a sender can log onto any public computer connected to the Internet, such as those in public libraries or Internet cafés and send encryption software anonymously to a recipient, who can also retrieve it anonymously. A would-be user of encryption software can anonymously download it from any of the thousands of Internet servers that openly provide a large collection of programs of this kind.

It may make sense for a country to ban the exportation of something that it alone possesses and that could be used against it, but it makes no sense for a country to ban the export of what other nations already produce locally. A 2004 survey by the Cyberspace Policy Institute of George Washington University, in Washington, DC, identified 4,723 encryption products (hardware and software) developed in 82 countries.

The study, published before the latest relaxing of U.S. export laws, explains that on average, the quality of foreign and U.S. products is comparable and that in the face of continuing U.S. export controls on encryption products, technology and services, some U.S. companies have financed the creation and growth of foreign cryptographic firms. With the expertise offshore, the relatively stringent U.S. export controls for cryptographic products can be avoided since products can be shipped from countries with less stringent controls.

Nevertheless, in recent years, the war over encryption has moved beyond the mere control of the technology itself. Although encryption proponents may have won the first round, law enforcement and intelligence agencies have responded with a slew of powerful tools for getting at computerized data (encrypted or not). These efforts are in turn being met by ingenious new schemes for hiding and protecting information, including one's identity.

ADVANCED HACKING

Today, as enterprise-wide networks reach the plant floor and zip data to the far side of the world in a twinkling, and, as the number of computers, personal digital assistants, telephones, and pagers communicating with the network increases, there is a corresponding increase in the opportunities for a critical blunder that would allow an attacker to enter your system. The consequences could be ruinous. According to a recent survey by the Computer Security Institute, the cumulative loss of 520 companies that quantified their losses in 2004 reached $712 million, or about $1.4 million each. Roughly $595 million of that loss was theft of proprietary information—information your competitors want.

One of the best places for plant engineers to learn about network security (see sidebar, "Hack Yourself Before Somebody Else Does") with a peer in information technology (IT) is at the Computer Security Resource Center, a Web site (*http://csrc.nist.gov/*) established by the National Institute of Standards and Technology (NIST). There you'll find primers that explain security issues and technologies, news about current problems and security initiatives, and downloadable copies of the standards that govern electronic communication with Uncle Sam. More than ever, it's vital that plant engineers work effectively with IT to identify potential breaches, shore them up, and train everybody to be security conscious.

HACK YOURSELF BEFORE SOMEBODY ELSE DOES

How do you test your system to make sure it's as safe as possible? Can you recommend software, hardware, or services that can identify security issues before they become problems? What kind of procedures do you have in place to make sure that the latest patches are applied to Web servers?

→

The best way to retain your network security is to do frequent security audits, including trying to gain access using easily available hacking tools. In addition, you should ensure that you only run the services you need and only open the ports needed by your network.

Your gateway to the Internet should be a system without any important company data or a hardware solution backed up by a firewall. You should also set up Windows Update notification for the server and have a backup server ready when you need to run the update.

Also, you should always check security bulletins and consider joining hacking mailing groups to find out what's happening on the other side of computer security. The main thing is to regularly test the security yourself; then you know what to find solutions for.

Nor is it only NIST that's getting into the act. The National Infrastructure Protection Center (*http://www.nipc.gov/*) was created by Congress to defend the nation's computer networks by serving as the national focal point for gathering information on threats to critical infrastructures. It is the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts. The center issues updates about new viruses, Internet frauds, and disruption attempts almost daily. It is located in the FBI's Washington headquarters and maintains its own investigative staff.

Cybersecurity isn't an exclusively local matter, however. A complaint filed by the U.S. Attorney for the Southern District of New York provides an instructive example of the reach of today's e-thieves. The complaint alleged that Oleg Zezov and Igor Yarimaka, residents of Kazakhstan, penetrated the computers of Bloomberg.com, in New York and demanded $200,000 from the company to tell how they had done it. Bloomberg agreed to pay, but only following a face-to-face meeting in London. There, accompanied by undercover London police officers, Bloomberg met with Zezov and Yarimaka. They repeated their demands, and police arrested them the next day. The United States is now seeking their extradition.

In view of the preceding incident, computer intrusions have more than tripled in the past two years. Who are the people trying to get their hands in your data, and why? Can you fight back by hacking yourself before somebody else does? This part of the chapter continues the theme of advanced computer forensics by providing answers to these questions.

Are We a Hacker Nation?

Shadowy, computer-wise predators slip in undetected to steal data, deface Web sites, crash systems, or just look around. Why? Because hacking has become nothing in recent years if not a good career move. Yesterday's hackers are today's security gurus, with more corporations counting on them for protection.

One reason there are so many types of hackers these days is that hacking—at least as manifested in its simpler forms such as Web page defacement and denial-of-service (DoS) attacks (which overwhelm a site with data to prevent users from accessing it)—has never been easier.

Tools of the Trade

The Internet is filled with Web sites that offer tips and tools for the neophyte hacker. Kids, criminals, and terrorists are some of the people who avail themselves of this information—so more and more intruders are knocking at port doors. The barrier to entering the hacker world has become very low. If you have a political motivation against wheat farmers and you want to deface their Web page, you could just go online and learn how to do it.

Despite tighter Web security and stricter penalties for breaking into systems, hacking attacks have more than tripled in the past two years. The government's Computer Emergency Response Team reported about 39,000 cases of corporate hacking in the United States in 2002, more than 40,000 cases in 2003 and over 62,000 in 2004, and those are just recorded cases. To avoid negative publicity, most companies don't report attacks. The statistics cover network break-ins (which can give a hacker access to data files), Web site vandalism, DoS attacks, and data theft. The FBI estimates that businesses worldwide lost $5.9 trillion in 2004 from security breaches perpetrated from within the business.

The risks are personal and professional: hackers can steal passwords and bank account numbers from your home PC or grab trade secrets from your company network. Recently, criminal hackers broke into Microsoft's corporate network and accessed source code for its software (see sidebar, "Future Threat: Advanced Malicious Code in Software").

FUTURE THREAT: ADVANCED MALICIOUS CODE IN SOFTWARE

Malicious code embedded in software is not new; users have always run the risk of downloading a virus or a trojan horse with shareware and games from the Net. The occasional intruder has even been found in shrink-wrapped products, but the hack into Microsoft's source code recently, raises worries that popular software may be the next target.

Although Microsoft indicates its code was not altered (the code was compared with previous backups) it's possible that a criminal hacker could get into a software manufacturer's code and insert a trojan horse. Unless software companies improve their security, you may find yourself the recipient of a gift horse in your next accounting package.

Hacking also poses risks for national security—sophisticated terrorists or hostile governments could conceivably crash satellite systems, wage economic warfare by interfering with financial transfers, or even disrupt air traffic control.

Good and Bad Hackers

Not all hackers have malicious intentions. Some hackers work for companies to secure their systems, and some contribute to security by notifying software vendors when they spot a vulnerability. Breaking things is easy. Building a solution is difficult, but arguably more fulfilling, but for every hacker who swaps his black hat for a white one, dozens of others continue to keep governments and companies on their toes.

Hacking will get worse. Bad software is being written faster than vulnerabilities are exposed. The trend is toward more features in applications, and the more features you have, the less security you get. Face it: hackers are not going to go away, so it's worthwhile to know who they are and why they do what they do.

Idle Hands

People see movies like *WarGames* and think hackers are going to start World War III. The truth is that computer hackers for the most part are smart, bored kids. Hackers usually start in their teens and stop by the time they're 30, but anyone can be a hacker—from the 16-year-old who defaces Web sites to the 36-year-old who sabotages a former employer's server. People in the underground indicate that not all hackers are true hackers.

By Any Other Name

It used to be that hacking had nothing to do with breaking the law or damaging systems. The first hackers, who emerged at MIT in the 1960s, were driven by a desire to master the intricacies of computing systems and to push technology beyond its known capabilities.

The hacker's ethic, an unwritten dictum governing the hacker world, indicates that a hacker should do no harm. A hacker should *pass through a network without a trace*. Somehow that message has gotten lost in the noise of Web defacements and data thefts.

Hacker purists get riled when anyone confuses them with crackers—intruders who damage or steal data, but although some hackers are quick to claim the moral high ground, the line between hacker and cracker is often blurred. Most hackers, for instance, don't believe it's criminal to break into systems and rifle around. The law, of course, thinks otherwise. Just because something is illegal doesn't mean it's wrong, but once you go in and destroy data or damage the system, that's where you stop being a hacker and you become a criminal.

T12, a 20-year-old who admits to some questionable hacking conduct, indicates he wouldn't normally damage a site, but if a phone company were to illegally switch his long-distance carrier and start billing his calls at $10 a minute, he wouldn't hesitate to take action. This is the kind of situation where one would feel free to just deface their site and make it as public as possible.

Diablo, a teenager with the Romanian hacking group Pentaguard, indicates that a hacker should never abuse his or her powers, but if you penetrate a server and change the main page, nobody is hurt. The administrator gets embarrassed, and that's all.

Pentaguard has defaced more than 100 Web sites (most of them government- and military-related) and Diablo indicates that he's careful: he never deletes or steals data and never crashes the system. This may be true, but the manager of one site Pentaguard defaced (owned by the Hawaii state legislature) indicated that his office had to pay $5000 for several new large-capacity hard drives (because the police confiscated the hacked hard drives as evidence), and the site was down for a week until the drives arrived.

Signs of the Times

Hacking has definitely changed in the past 43 years. Talk to any hacker over 25, and he's likely to lament the passing of the good old days, when coding was an art form and learning how systems worked was an exercise in persistence. They say new hackers today are often younger and less skilled than their predecessors and more likely to focus on showy exploits than the noble pursuit of knowledge.

Many old hackers call the Internet generation of hackers *hollow bunnies*—such as gigantic chocolate Easter bunnies *filled with nothing but air*. Ten years ago, hackers respected information and machines and had to possess knowledge and skills to hack. Now novices use hacking programs without understanding them and are more likely to leave havoc in their wake.

Script kiddies receive the bulk of hacker disdain. These are the graffiti kids who download canned scripts (prewritten hacking programs) for DoS attacks or paint-by-number Web defacements. The risk here is that an unskilled hacker could release wanton mayhem in your systems. The hacker might download a buggy hacking tool to your network that goes awry or execute a wrong command and inadvertently damage your machines. But script kiddies tend to disappear after a year. This is the generation of instant gratification, and if they can't get the hang of Back Orifice (a more advanced hacking program), they get bored and move on.

Bigger Threats

Script kiddies may get attention, but experts agree that the most dangerous hackers are the ones who don't make any noise: criminal hackers and cyberterrorists.

The truly dangerous people are hacking away in the background, drowned out by the noise and pomp that the script kiddies and DoS packet monkeys have been making.

Hacking has evolved into professional crime. Amateur hackers are falling into the minority, and now the fear is the criminal and the terrorist. These are people like the Russian cracker group that siphoned $20 million from Citibank in 1994 and the mafia boss in Amsterdam who had hackers access police files so he could keep ahead of the law.

In 1997, crime syndicates approached hackers to work for them. Now, with so many easy-to-use hacking tools on the Internet, criminals hardly need hackers to do their dirty work.

The cyber element that everyone fears most is one you've yet to see: foreign governments, terrorists, and domestic militia groups hacking for a political cause. The Department of Defense indicates its systems are probed about 583,000 times a year. It's difficult to tell if probes are coming from enemies seeking military data or from "ankle biters"—harmless hackers on a joyride. Regardless, authorities have to investigate every probe as a potential threat.

The likelihood of obtaining top secret information in this way is small, because classified data is generally stored on machines not connected to the Net. A more problematic assault would focus on utilities or satellite and phone systems. Ninety-two percent of U.S. military communications run through civilian phone networks. An attack on these systems could impede military communications.

For example, Navy officials recently reported that hackers broke into a Navy research facility in Washington, DC and stole two-thirds of its source code for satellite and missile guidance systems. The Navy indicates that the source code was an unclassified older version.

Thus, a large-scale cyberattack is imminent. Members of terrorist groups such as Hezbollah have been educated in Western universities and are capable of developing such attacks in the future—such as a digital 9-11 attack.

Why Hackers Hack

Aside from criminal and political motives, the reasons that hackers hack range from malice and revenge to simple boredom. Despite the image of hackers as dysfunctional loners, many are drawn to hacking by the sense of community it gives. Of course, a big part of hacking's attraction is the sense of power that comes from uncovering information you shouldn't possess. A hacker called Dead Addict once described the high that comes from discovering valuable information, followed by the low that comes from realizing you can't do anything with it.

For example, one hacker knows a little of that rush. He says that he once broke into a hazardous waste firm and found *pretty evil insider information* that no one was meant to see. Though he didn't act on the information, he did log it for possible use later—just in case he felt like being socially active.

Many hackers who begin as system voyeurs graduate to more serious activities. It's easy to be lured to the dark side when you get easy gratification messing around with individuals such as for example—AOL users. Most hackers are not old enough to drive a car or vote, but they can exert power over a network.

White Hats

There are a lot of the reasons why hackers' ability to hack into computers fade with age. Life fills their time and their ethics begin to change. The majority eventually find their interest waning. You only have three directions to go with hacking: you can keep doing the same old tricks, you can become a real criminal cracker, or you can use those skills wisely to build new software and create a more secure Internet.

Securing the Net is an interest many hackers develop (especially now that employers are hiring them for their skills). They lament that the public never hears about their positive acts, such as patching a hole on their way out of a site and letting the administrator know they fixed it. Most companies just focus on the fact that you hacked them and want to come after you with a lawsuit. It's made hackers reluctant to help them.

An even sorer point between hackers and vendors is the issue of releasing vulnerability exploits. These are findings about a security problem that hackers (and researchers) post on the Net. Vendors indicate hackers expose the holes for anyone to exploit and should instead report them to vendors first so they can fix them. The hacking community frowns on people who don't notify vendors, but when they do, vendors often ignore them. Most software companies won't do anything about a problem until you make it public. Then they have to fix it.

Vendors have a duty to develop secure software. Hackers, on the other hand, force vendors to admit their errors after they've hacked into their software. Manufacturers are grossly negligent in selling software that doesn't stand up. What if they were producing cars that were this unsafe? The software they give us is not safe to drive in cyberspace.

Anything that's attached to the Internet is potentially hackable, and if you're using a Windows 2000, XP, or 2003 machine, nothing that is on that computer is secure. Better security is in everyone's best interest, and hackers should play a crucial role in this. The hacker kids who are going to Def Con today are the software architects of tomorrow. The same thing that makes them hackers makes them valuable to employers in the future.

All of this points to the fact that although hackers may be the Internet's greatest annoyance, their warnings are ignored about security at everyone's peril. The network that can't guard against a bored 18-year-old hacking in his or her spare time, can't hope to protect itself from a hostile government or tech-savvy terrorist.

ADVANCED TRACKER HACKERS

As the number of computer crimes spirals, the computer forensics experts' (a rare breed of security pros) skills are getting ever more precious. These are the data detectives who search for digital clues remaining on computers after malicious (or black-hat) hackers have done their dirty deeds. Cyber sleuths analyze email, Web site records, and hard drive data, looking for clues to the identity of criminals and crackers, much like gumshoes examine crime scenes for fingerprints and stray hairs.

It's not only the number of crimes that's fueling the need for these skills but also the increasing sophistication of criminals. The black-hat community is moving forward at a pace that outstrips the ability of the average system administrator or law enforcement agency. That means that both e-businesses and law enforcement agencies are paying plenty to find experts to sift through evidence left behind at digital crime scenes.

In other words, security consultants and auditors are well-compensated for their knowledge—especially since the 9-11 attacks. In a recent survey of more than 11,000 IT managers, security consultants, on average, make $20,000 more per year than network administrators. Overall, salaries for all positions grew 33.9% to an average of $109,176 in 2004 (see Table 20.1).

TABLE 20.1 The Salary Protection Racket

Position	*Average salary*	*Increase from 2003*
Security consultants	$121,783	+23.7%
Security auditors	$110,722	+26.7%
Security administrators	$101,368	+29.9%
System administrators	$108,313	+44.3%
Network administrators	$104,047	+45.1%

The need for computer forensics is growing exponentially. The need is particularly acute at local, state, federal, and military law enforcement agencies that host computer forensics divisions, which are looking for individuals adept at solving hacking and intellectual property cases. An increasing number of corporations are using computer forensics to resolve internal matters such as fraud, violations of trade secrets, and inappropriate use of company computers.

The job is intense and tedious and requires nerves of steel. Most specialists have years of programming or computer-related experience, strong analytical skills, and the patience to invest days taking apart a computer in search of evidence. If things keep going the way they are, it probably won't hurt if these experts don't mind overtime.

Other professional attributes needed to catch a thief are strong computer science fundamentals, a broad understanding of security vulnerabilities, and strong system administration skills. Cyber sleuths use these skills to seek information to reconstruct how a system was hacked. The number and complexity of intrusions has increased at an alarming rate. Cyber sleuths have been forced to find ways to try to keep up with intruder tools as they have progressed in sophistication.

Experts gather this data and create an audit trail for criminal prosecutions. They search for information that may be encrypted or hidden, along with unallocated disk space. Most cunningly of all, they set traps using vulnerable computers to lure malicious hackers into giving away themselves and their techniques.

Computer forensics specialists must have strong analytic skills and excellent verbal and written communication skills. That's because they're required to document their findings in detail, and they often testify at criminal trials.

The demand is being answered by several educational facilities, including the University of Central Florida, in Orlando, which offers a graduate certificate degree in computer forensics. The International Association of Computer Investigative Specialists, based in Donahue, Iowa, offers certification for computer forensics examiners. Demand for such courses is so high that the association's fall classes are already full. Such courses are helpful for IT managers or individuals who lack computer programming experience but who want to make the leap into computer forensics.

Computer forensics specialists caution that IT managers interested in pursuing computer forensics as a career shouldn't expect that just by taking a few courses in the subject, they'll be able to track some of the world's slyest hackers (see sidebar, "The Costs of Tracking a Hacker"). The specialty is a tough discipline in a fast-moving industry that requires highly trained professionals dedicated to continued learning. That's because there's no way to stay ahead of the crooks. White-hat hackers at this point can only try to narrow the gap between themselves and the bad guys—and hope that the black-hat hackers don't get too fastidious when it comes to leaving behind digital footprints.

THE COSTS OF TRACKING A HACKER

It took the intruder less than a minute to break into the university's computer via the Internet, and he stayed less than a half an hour, yet finding out what he did in that time took researchers, on average, more than 34 hours each.

→

That inequity—highlighted during the Forensic Challenge, a contest of digital-sleuthing skills whose results were announced recently—underscores the costs of cleaning up after an intruder compromises a network. That damage done in a half an hour would take a company an estimated 34 hours of investigative time and cost about $3,000 if the investigation was handled internally and more than $33,000 if a consultant was called in—and those are conservative estimates.

Eventually, the members of a loose group of security experts known as the Honeynet Project, announced the winner of the Forensic Challenge. The contest pitted the reports of 13 amateur and professional cyber sleuths against one another.

Each digital detective used decompilers, data recovery programs, and other forensic tools to uncover as much information as possible. The entries consisted of a memo to fictional upper management, a security advisory, and an in-depth analysis of the evidence uncovered by the contestant's digital detective work. The winner of the contest, Thomas Roessler, a student in mathematics at the University of Bonn in Germany, has dabbled in, but not done digital forensics work in the past. Roessler indicated that it's always amazing how much information you can get out of a system by using rather basic tools. You always miss something.

The contest was made more interesting by the fact that the attack was a real one, captured by one of the several "honeypots" (vulnerable computers connected to the Net and surreptitiously watched) run by the Honeynet Project. In fact, the detectives produced several leads to the identity of the culprit. However, the person responsible would not be prosecuted. Such on-line vandals are extremely common.

The perpetrator represents a very large and common percentage of the black-hat community. It's a threat that everyone faces. Nevertheless, only about 70 to 80% of the so-called black-hat hackers (those who break into computers illegally) have comparable skills to the attacker who breached the computer.

The contest also helped illuminate why securing a computer is more cost-effective than hiring consultants to come in and do the detective work afterward. It is a fairly extensive process to take what amounts to a bunch of garbage and build a comprehensive picture of what happened. The costs of such investigations can easily amount to $63,000 per computer.

Companies need to understand the difficulty, and costs, involved. Companies also tend to balk at agreeing to that kind of expense when there is no guaranteed payoff. Maybe the contest opened the eyes of corporate executives, who all too often want a quick fix.

If you just reinstall the system, do you know if you have plugged the hole that allowed the attacker to get in? Most of the time, such quick fixes just mean the attacker gets another shot at the system. Some computers at the University of Washington have been compromised five times. Multiple intrusions are occurring all over the place.

→

The Honeynet Project plans to do another contest soon, but it's a question of time. The next project would also focus on either a Solaris or Windows NT/2000, XP, or 2003 computer.

Anonymity in Retrieving System Logs

The 9-11 terrorist attacks have had numerous effects on national security. One of these is legislation that increases the ability of federal agencies to intercept Internet traffic. Another side effect was the loss of the well-known Web anonymity service hosted by ZeroKnowledge, which turned out not to be related to any of the national security activities during 9-11.

Web anonymizers allow people to visit Web sites without disclosing their identities to the owner of the Web site, or even a local administrator who can log the URLs that a user visits. These tools work just as well for a terrorist who wishes to use the Web with anonymity, although using Internet access in a Web café, which one of the plane hijackers did, works well, too.

Anonymity has its place in a free society, and personal rights and freedoms shouldn't be collateral victims of terrorist attacks. Interestingly, government agencies may also be important users of anonymizers. This section explains how anonymization works on the Internet and why this is important in the face of increasing privacy concerns.

Source Addresses

A source address is an IP address embedded in the header of an IP packet. When the packet is received, the source address becomes the destination address in the reply packet. If you spoof your source address, reply packets wind up going to the address that you've spoofed, and you don't see the results. Worse, spoofing your source address is a lousy technique for anonymity, as most application protocols require a completed transmission control protocol (TCP) connection before exchanging any information.

Something similar to source address spoofing occurs whenever a firewall is between you and the destination network. Most firewalls translate internal addresses into external addresses, most commonly through network address translation (NAT). Another way to rewrite the source address is to connect to a proxy and ask it to connect to the server you want to visit. This capability is built into Web browsers, which permits you to specify the IP address and the proxy you wish to use. If you've configured your Web browser to use a proxy, the Web server sees the address as the source. The proxy relays for you transparently.

Of course, whoever maintains the proxy or firewall has logs of your activity. And the owner of the Web server still has information about you—for example, the type of Web browser you're using, the source IP address, the URL requested, any referring page, as well as the source operating system, and sometimes the type of PC.

The Web site's operator can go farther still: a Web designer can include Javascript to collect more information about your browser and operating system, attaching that to any form data that you return. This information may include your system's real source IP address, which is accessible to Javascript programs.

Routing to the Rescue

Surprisingly, the U.S. Navy has researched network anonymity. This research formed the basis for the Freedom Network and may show up in other systems for anonymity as well.

Suppose that you proxy your Web requests through a third party who promises to keep its logs a secret. You connect to this server via secure sockets layer (SSL) so that anyone sniffing the connection can only see that you're visiting an anonymizer, and not your final destination site, which is encrypted. Sounds like a reasonable solution, but it hasn't worked in the past.

In the early 1990s, a site in Finland, *anon.penet.fi*, provided an anonymous remailer. Anonymous emailers strip away revealing information from email headers before resending it to your intended destination. That works well as long as the software manages to remove all the headers and you don't include revealing information in the email you send (for example, including an automatic signature file at the end of your email that, consequently, identifies you).

Penet also supported using aliases, so that the person receiving your email could reply to you without learning your identity. Therefore, Penet had to keep track of the mapping between your anonymous email address and your real one. Penet worked well until authorities stepped in and demanded that Johann Helsingius, Penet's operator, disclose the mapping of a particular email address because it involved information copyrighted by the Church of Scientology.

If the proxy doesn't even know your real source address, how can it successfully relay for you? There have been several approaches to this problem, and one of the most recent (as previously discussed) is Onion Routing.

In Onion Routing, instead of having a single proxy for relaying, there's a network of proxies. Each of these proxies runs the same software, which not only relays your packets but also encrypts them. The first Onion Router chooses a route for your connection, then encrypts your data several times, each time using the public key for one of the routers in its network of routers.

This is where the "onion" comes in. Each layer of encryption resembles the skin of an onion: the Onion Router you've connected to first encrypts your data using the key of the last router in its list of routers—this makes up the innermost layer of the onion. Once this layer of encryption is removed, the packet is sent to its real destination. Then, the first Onion Router adds another layer of encryption. This layer includes the address of the last router in the list, and gets encrypted with the second to last router's key. The next layer gets added, with the address of the second to last router's address, but using the third to last router's key, and so on. There should be at least six routers to ensure confidentiality.

Onion Routing is even more effective if you run one of the routers. Your Onion Router must also be a full participant in the network, so that other Onion Routers can use it. Otherwise, packets coming from your Onion Router will only contain packets from your network, and can reveal your approximate source, even with the content still encrypted.

Onion Routers present another potential problem. An aggressive attacker could monitor the network traffic of every participating Onion Router. This attacker (or snoop) can then track traffic patterns. For example, you send off a request to *http://www.fbi.gov* via your Onion Router. The snoop sees traffic leaving your Onion Router, bound for another Onion Router, with a certain packet size. The next router sends off a slightly smaller packet and so on, until the final router sends the plaintext packet directly to the real destination. Then the snoop can deduce that this packet came from your network, based on the sizes and the timing of the packets between routers.

Onion Routing defeats this by delaying packets slightly, as well as batching data from several packets. Thus, a snoop cannot make simple deductions about the size and timing of packets. The end user does experience greater latency (delay), but this is the price for greater security.

Onion Routing is only one approach to the problem of network anonymity. AT&T Research (*http://www.research.att.com*) tried a different approach called Crowds. The concept behind Crowds is that "anonymity loves company," so the more participants the better. Each Crowd proxy is called a "jondo" (think "John Doe"). Unlike Onion Routing, which relies on layers of encryption, jondos employ secret key encryption with one key per route. This speeds up processing by reducing the amount of time required to handle encryption. As with Onion Routing, state information is required so that the entry and exit points of a route know where to send packets. This information is discarded at the end of each connection but could be used to track users.

The Freedom Network used an approach similar to Onion Routing. You could either add a plug-in to Internet Explorer or patch your Linux kernel so that your system actually becomes an entry point in the network, with sites other than the one run by ZeroKnowledge participating as routers. The Freedom Network claims that it decided in spring 2001 to discontinue its service because it wasn't paying for itself.

As of this writing, the Anonymizer (*http://www.anonymizer.com*) is still up and running but functions as a proxy; it also strips identifying information from your requests. Although you can use this service for free, your request will be delayed so that you can read ads encouraging you to pay for the service.

You can also acquire software that acts as a local proxy for Web requests. This software removes the USER-AGENT line and strips away cookies, which can also be used to track your use of a Web site.

Who Needs It?

The Onion Routing project closed down in January 2000, after processing over 30 million requests. Its home page contains an interesting disclaimer, essentially saying that anyone using the Navy's network should expect their traffic to be monitored—a very chilling statement when one considers the alleged intent of Onion Routing.

Still, government agencies form one of the largest groups of anonymizer users. Anonymizers allow law enforcement to visit Web sites without giving away their identity, or military analysts to collect data without revealing their areas of interest. Such uses of anonymizers are legitimate and actually of value to national security. If only the military and law enforcement used a particular anonymizer, then any visits from that anonymizer would immediately be of interest to someone worried about being investigated.

Anonymizers also have a place for nongovernmental users. While an anonymizer has the potential for misuse—for example, by hiding the identity of visitors to a pornographic site with illegal content—anonymizers have historically had more important and legitimate uses. For example, someone with AIDS could feel free to search the Web without revealing his or her identity. A person on the verge of committing suicide could ask for help, while remaining anonymous, which was one of the actual uses of the original Penet remailer. One can only hope that the rush to embrace national security in the United States doesn't have additional casualties—especially ones that actually enhance national security.

Denial of Service

Pity the poor intrusion detection system (IDS)—it has the reputation of an irritating snitch and the track record to prove it. Perhaps no other security device has done its job so well and then been reviled so roundly for doing it. Designed to sniff out and warn system administrators when hackers are trying to exploit network vulnerabilities or launch denial-of-service (DoS) attacks, the original IDSs did their job all too well. That was both bad and good news.

True to vendor promises, first-generation IDSs generated information-traffic patterns on network segments, aberrations in host log files, and so forth, which could indicate whether their systems had been hit with any of the attacks hackers use to break into critical network resources. This required placing IDSs at key locations on the network, such as at firewalls, switches, routers, Web servers, databases, and other back-end devices further into the enterprise—a straightforward process.

Those IDSs were also overly chatty boxes, renowned for generating mountains of data on traffic passing through networks and on host systems. They cried "wolf" too often, reporting false alarms by the droves. Consequently, many systems administrators, overwhelmed by tons of information they couldn't digest or didn't understand, simply dumbed them down or shut them off entirely.

The IDS products on the market are now bigger, better, and faster and offer much more to those charged with protecting network resources. Vendors have, for instance, developed new intrusion detection methods that go beyond the pattern, or signature-matching, technology that plagued the earlier products with all those false alarms. They have also increased the performance of their devices, which can now keep up with 100 Mbit/sec networks. Vendors are also shipping appliance-like IDSs, which simplify their deployment and management, and they've begun delivering products that combine the best of the two principal types of IDSs into a single offering.

Just as importantly, the number of attacks on networking systems is growing. It's a jungle out there, and network managers need to keep the predators at bay with a variety of security devices, including the IDS. For example, the nonprofit CERT Coordination Center received reports on 44,304 security incidents in 2004 (the most recent year for which its incident totals are available). That's comparable to the 33,879 it received in 2003, and the 22,768 incidents logged for 2002.

The most virulent threat to emerge from the hacker jungle, though, is clearly DoS and distributed DoS (DDoS) attacks, the number and variety of which have increased dramatically according to security organizations. Hackers target DoS attacks at devices and networks with Internet exposure, especially e-commerce sites [4], according to the National Infrastructure Protection Center (NIPC). The goal of such attacks is to incapacitate a device or network with bandwidth (devouring traffic so that external users can't access those resources)—this without hacking password files or stealing sensitive data.

In March 2004, NIPC continued investigating a series of organized hacker activities that specifically targeted e-commerce and online banking sites. NIPC identified 500 victims in 33 U.S. states who were attacked by organized groups in Eastern Europe (particularly Russia and the Ukraine), which took advantage of vulnerabilities in servers running an unpatched version of Microsoft's Windows NT operating system. Once the Eastern European hackers gained access, they downloaded a variety of proprietary data—mostly customer databases and credit-card information. In this case, the intruders didn't use the information maliciously, per se, because they didn't attempt to make purchases with the stolen cards. They did, however, make veiled extortion threats by offering to furnish paid services that would "fix" the unpatched systems.

A Second Look

It's thus time for network professionals who gave up on the IDS a few years ago to go looking again. Indeed, market research numbers indicate that more and more of them plan to deploy IDSs in the coming years. Frost & Sullivan, for example, predicts that the market for intrusion detection software will increase from $665.6 million in 2004 to $887.8 million in 2006 and $998.9 million in 2007. Another research house, IDC (*http://www.idc. com*), paints a slightly rosier picture, saying that the IDS market stands at $1 billion in 2005 and will grow to $5.6 billion by 2006.

Several developments have moved the IDS back into prominence. These include IDSs' new ability to keep up with the high-speed transport technologies found in today's networks, the emergence of IDS "appliances," new intrusion-detection methods, better management tools, and a hybrid approach that combines the monitoring of the network- and host-based systems, the two basic types of IDSs, with a single console. The charge is led by many of the usual vendor suspects—Cisco Systems [5], Internet Security Systems (ISS), Intrusion.com, NFR Security, and Symantec—as well as numerous newcomers. The latter list includes CyberSafe, Entercept Security Technologies, and Enterasys Networks.

The market has also spawned a growing number of managed security services providers (MSSPs) with outsourced offerings that include intrusion detection capabilities. In this area are Activis, Exodus Communications, OneSecure, NetSolve, RedSiren Technologies, Riptech, and Ubizen.

Moving to Anomoly Tracking

As noted, the developments driving the IDS marketplace are improving organizations' ability to monitor and secure against unwanted attacks, whether intrusions or DoS/DDoS strikes. Arguably, the most critical is the growing use of anomaly-based intrusion detection by vendors of network-based IDSs.

The traditional network-based IDS discovers malicious traffic by detecting the presence of known patterns, a process usually called "signature matching." These systems work much like an anti-virus software package (detecting a known "bad" pattern generates an alarm) and effectively discover known patterns.

On the downside, signature-based network IDSs can suffer on two principal accounts. First, they can't see inside encrypted packets—the encryption essentially hides the packet's contents from the IDS, leaving it blind to assaults. Second, hackers often mutate the nature of their attacks, rendering pattern-matching useless. Just as an anti-virus package can't protect against a new virus until vendors patch their software, an IDS vendor must update its signature files—and it's not clear how many vendors have figured that out.

The anomaly-based network IDS uses packet sniffing to characterize and track network activities to differentiate between abnormal and normal network behavior.

These devices analyze the data transfer among IP devices, permitting them to discern normal traffic from suspicious activity without pattern or signature matching.

These devices don't care about the content of data in a session (as with signature matching). They only care about how a session took place, where the connection was made, at what time, and how rapidly (is a suspicious connection to one host followed by a suspicious connection to another host?).

With anomaly-based systems, it's important to get a baseline of what "normal" network traffic looks like. The chief difficulty of this approach is how to baseline—to know what's normal traffic as opposed to deviated. Signature-matching should be coupled with anomaly tracking. An anomaly can be compared against a signature, and if the anomaly doesn't show up on multiple probes, you ignore it. Cisco Systems, Enterasys Networks, Lancope, Intrusion.com, ISS, and Recourse Technologies are among the vendors that offer anomaly-based network IDS products.

Faster Systems

Most IDSs on the market now can keep up with a 400 Mbit/sec Ethernet. Beyond that, they begin to drop packets and become less efficient. When vendors push their IDS offerings beyond 400 Mbits/sec, they're only looking at a subset of packets. You can find products that will die in 400 Mbit/sec networks. Other players that boast IDSs capable of operating in 400 Mbit/sec network environments are Cisco and Enterasys.

Moving to Appliances

Another trend among IDS products is the network-based IDS appliance. Unlike first-generation IDS products, which required installing and configuring the vendor's intrusion-monitoring software on a PC, these appliances merge hardware and software into a preconfigured unit.

Cisco's Secure IDS, formerly known as the NetRanger, was among the first such appliances, and IDC believes this makes Cisco the current leader in this area. ISS (working with Nokia), Intrusion.com, and NFR Security (formerly Network Flight Recorder), are also moving their IDS products into the appliance category.

The appliance approach makes sense for several reasons. First, it eliminates many of the performance issues involved in installing IDS software on a general-purpose PC. The IDS software vendor can't optimize its product for every processor and revision of operating system. Second, the appliance is a controlled environment, built to vendor specifications, so the IDS software can be configured specifically for the application. Appliance-based IDS boxes also eliminate operating system–related concerns, especially in all-Wintel or all-Unix organizations. Finally, appliance-based IDSs give plug-and-play capabilities to IT departments in multilocation companies and to service providers. These are especially valuable for deployment in remote offices, where novice end users can handle the physical connections while leaving setup and configuration to centralized IT staff.

IDS vendors have developed recent products that merge the capabilities of host- and network-based systems into a single management platform. In these environments, a management console works in conjunction with traffic- and log-analysis tools on the network and host IDS systems to provide a correlated view of network activity.

Correlating data from multiple network sources lowers the incidence of false positives and enables network security personnel to view traffic from a higher level. For instance, a single scan of Port 80 on a Web server via a single router probably would not reveal the presence of an attack, but multiple scans across several routers would.

Outsourcing Intrusion Detection

Advances in IDS technology notwithstanding, organizations worried about unauthorized intrusions and DoS attacks should also consider outsourcing their intrusion detection needs. Outsourcing intrusion detection to an MSSP, which monitors customers' IDSs via the Internet, can make sense for several reasons. Not the least of these is cost. Companies with small, limited staff with limited experience in security can benefit greatly from an MSSP. It would typically require five employees, working three eight-hour shifts (with extra staffing for vacations, sickness, and the like), to handle the 24-by-7 needs of an IDS-monitoring program. Forget about the $50,000 for the IDS—an employee costs at least $90,000 a year, and with five employees, you could spend a fortune on training and maintaining security personnel.

Thus, it's important to sit down and perform a return on investment (ROI) study. During this process, IT organizations should ask themselves whether they have the expertise to operate critical systems that can cost a business revenue or customer confidence if they're compromised as the result of hacking or DoS or DDoS attacks.

The MSSPs tout the level of security expertise among their employees, claiming that this expertise enables them to better handle the task of deciphering often arcane IDS logs and alarms that befuddle typical IT employees. In addition, MSSPs have often deployed tools specifically designed to acquire and correlate information from a wide range of intrusion detection devices and systems. MSSPs Riptech and OneSecure, for example, both indicate that the technology they've developed in this area differentiates them from others in the market.

Riptech, for instance, spent two years developing proprietary data-mining and correlation software for its Caltarian security service. Caltarian's software permits the company to warn clients of attacks while they're under attack, with recommendations to protect their networks in real time.

So, perhaps one shouldn't pity the IDS after all. No longer an overly chatty box crying "wolf" too often, it now offers network managers an improved set of tools that can finally help them fend off unwanted attacks from insiders and outsiders alike.

Signs of Attempted and Successful Break-Ins

Hackers are succeeding more and more in gaining root-privilege control of government computer systems containing sensitive information. Computers at many agencies are riddled with security weaknesses. When an attacker gets root privileges to a server, he or she essentially has the power to do anything that a systems administrator could do, from copying files to installing software or sniffer programs that can monitor the activities of end users.

The increase in the number of root compromises, DoS attacks, network reconnaissance activities, destructive viruses, and malicious code, coupled with the advances in attack sophistication, pose a measurable threat to government systems.

In 2004, 599 systems at 43 federal agencies suffered root compromises in which intruders took full administrative control of the machines, according to the General Services Administration (GSA). That's up from 186 root compromises in 2002 and 332 in 2003. The government has only a vague idea of what kind of data may have fallen into the wrong hands.

For at least five of the root compromises, officials were able to verify that access had been obtained to sensitive information. For the remaining 594 incidents, compromise of any or all information must be assumed. The compromised data involves scientific and environmental studies.

Meanwhile, the U.S. General Accounting Office (GAO), in a report recently released, summarized security audits that have been completed at 35 federal agencies and indicated it had identified significant security weaknesses at each one. The shortcomings have placed an enormous amount of highly sensitive data at risk of inappropriate disclosure.

The government is going to find itself in "deep, deep trouble" if its IT security procedures aren't improved. If sensitive personal data about U.S. citizens is compromised, Americans are going to wake up angrier then you can possibly imagine.

Many of the thousands of attempts to illegally access federal systems come from abroad. Also, many nations are developing information warfare capabilities as well as adapting cyber crime tools. Hackers exchange vulnerability information with one another. There is a whole new currency on the Internet that's called the back door. Attackers trade information about back doors that provide access to different systems.

One step the government could take to increase the security of its systems is to focus more resources on improving education and training. Computer security experts are scarce. They are in short supply, and they are expensive. The average salary is $120,000.

A 1998 directive by President Clinton, ordered all federal agencies to complete a virtual bulletproofing of their IT systems from attack by May 2005, but officials indicate that most agencies are behind in that work, and only a few are doing penetration testing.

Even more alarming, is that many attacks aren't detected. No one knows what was done, and no one has a way of knowing what was done.

Forensics

Threats to an enterprise's information infrastructure can come in a number of unsuspecting forms. Beyond fending off network intrusions and DoS attacks, companies must stave off threats of industrial espionage.

Layoffs occur more frequently these days, and when the disgruntled, newly disenfranchised leave, today's technology makes it easy for them to sneak off with trade secrets, research materials, client lists, and proprietary software. Increasingly, cyberthieves are raiding corporate servers, electronically stealing intellectual property, and using email to harass fellow employees, putting companies at risk for liability. The impact on the bottom line alone is cause for concern; the American Society of Industrial Security reports that theft of intellectual property in the United States costs businesses almost $6.9 billion annually.

Constant developments in information technology have posed challenges for those policing cyber crime. For many organizations, identifying, tracking, and prosecuting these threats has become a full-time job.

Specialists in computer forensics must use sophisticated software tools and spend enormous amounts of time to isolate anomalies and detect clues for evidence of a cyber crime or security breach. As previously explained, computer forensics is the equivalent of surveying a crime scene or performing an autopsy on a victim. Clues inadvertently left behind after a cyber crime can often be pieced back together to reveal details of wrongdoing and eventually pinpoint the perpetrator.

Although software tools can identify and document evidence, computer forensics is more than just technology and analysis. Safeguards and forensics methodologies ensure that digital evidence is preserved to withstand judicial scrutiny and to support civil or criminal litigation should the matter be brought to trial.

Divining Good Forensics

Obtaining a good digital fingerprint of a perpetrator requires that steps be taken to preserve the electronic crime scene. The systematic search for evidence must adhere to basic guidelines to prevent the inadvertent corruption of original data during the course of investigation. Even booting up or shutting down a system runs the risk of losing or overwriting data in memory and temporary files.

The examination will usually begin with a look at the disk drive. Minimal handling preserves its integrity, so any disk investigation should begin by making a copy of the original, using the least intrusive manner available.

Today's forensic software tools can sniff out storage areas for data that may otherwise go unnoticed. Ambient system data, such as swap files and unallocated disk space, and file "slack" (data padded to the end of files), often hold interesting clues, including email histories, document fragments, Web browsing details, and computer usage time lines.

Be careful to document any inadvertent changes that may occur to the original drive data during data extraction. Complying with the rules of evidence preservation and upholding the integrity of the process will help prevent any future challenges of admissibility.

Although somewhat trickier than hard drive examination, data communication analysis is another useful forensic tool. Data communication analysis typically includes network intrusion detection, data preservation, and event reconstruction. Isolating suspicious network behavior also requires the use of specialized monitoring software. Doing so can reveal activities such as unauthorized network access, malicious data-packet monitoring, and any remote system modifications.

Leave It to the Pros

Although today's sophisticated data-recovery tools have become fairly efficient, the process of recovery remains a tedious, labor-intensive task. And no matter how good the tools, the science of computer forensic discovery draws on multiple disciplines. Forensics demands a skill set often composed of software engineering and a solid familiarity with binary systems and memory usage, disk geometries, boot records, network systems, and data communications. Principals of cryptography are also important for identifying data encryption and password-protection schemes. Only experience can teach a forensic examiner how to avoid booby traps or an extortionist's logic bomb—items often left to wreak havoc along the path to discovery if not properly dismantled.

For these reasons, it's often wise to leave the process to the professionals. An expert in forensics will be able to quickly isolate the telltale signs of where to look for clues and will better understand data-discovery technologies as they apply to the legal process.

When selecting a forensic examiner, you should have several goals in mind: Your candidate should be familiar with the intricacies of your particular operating systems, know how to protect against data corruption and booby traps, and have a history of court appearances and controls established to deal with evidentiary procedures, such as chain-of-custody.

If you're looking for more information on computer forensics or getting your staff trained on good procedure and practice, there are a number of good resources at your disposal. As storage capacities and network sizes continue to increase, so do the means by which cyberthieves can circumvent security as well as the effort required to bring them to justice. So start training to detect the signs of suspicious activity today and learn how forensic computer investigation can protect your corporate assets in these dangerous times.

How a Hacker Works

Obviously, knowing how the hacker's mind works is only half of the battle. You must also know your network inside and out, identify its vulnerable points, and take the necessary steps to protect it. This section will look at some tips and tools administrators can use to prevent those vulnerabilities.

Diagram Your Network

You should begin by diagramming the topology of your network. You can do this with a sophisticated tool such as Visio, or you can use a less complex tool such as Word. Simpler yet, you can draw it by hand. Once you've diagrammed your network, identify all the machines that are connected to the Internet, including routers, switches, servers, and workstations. Then, evaluate the security precautions in place on those machines. You want to pay close attention to machines that have a public IP address on the Internet, because they're the ones that will be scanned by hackers.

Always-On Means Always-Vulnerable

Currently, the greatest security vulnerability is always-on Internet access using static IP addresses. With always-on access and a static IP, you are a like a big bull's-eye sitting on the Internet waiting to get hit. The question is, once hackers get in your network can they do any damage, or will they be frustrated and move on to the next target? If you have an always-on Internet connection, you should already have a basic security policy and firewall in place on your network. If you have a Web server, mail server, or other servers constantly connected to the Internet, your security responsibilities are even greater. Because the Internet is built upon the TCP/IP protocol, many hacker attacks will seek to exploit the TCP ports of these servers with public IP addresses. A number of common ports are scanned and attacked:

- FTP (21)
- Telnet (23)
- SMTP (25)
- DNS (53)
- HTTP (80)
- POP3 (110)
- NNTP (119)
- IMAP (143)
- SNMP (161)

NOTE

You need to identify whether your servers are utilizing any of these ports (the numbers above in parentheses) because these represent known vulnerabilities.

Ways to Protect the Network

There are a number of ways to compensate for these vulnerabilities. First, you can implement firewall filtering. One of the best protections against port attacks is to implement a firewall with dynamic packet filtering, also called "stateful inspection firewalls." These firewalls open and close ports on an as-needed basis, rather than permanently leaving a port open where it can be identified by one of the hackers' port scans and then exploited. You can also analyze your system log files to track hacker activity. A third option is to install an intrusion-detection program that will do much of the log file examination for you.

Seeing What the Hacker Sees

In addition to protecting against the well-known vulnerabilities, you need to see what the hacker sees when he looks at your network. The best way to do this is to use nmap, a program that gives you a look at your network from a hacker-like perspective. A company called eEye has released a new version of this program for Windows NT (you can download it at *http://www.eeye.com/html/Research/Tools/nmapNT.html*). The company also offers an industrial-strength network security scanner called Retina, which helps discover and fix known and unknown vulnerabilities. This is an expensive, yet valuable, product.

NOTE

You can download the Linux version of nmap at http://www.insecure.org/nmap/.

Software Vulnerabilities

Hackers also often exploit software security problems. They take advantage of these behind-the-scenes parts of the software to gain access to your system. Thus, you should take stock of all the software running on your Internet-exposed systems. Go to the Web sites of the vendors that make each of the software packages and bookmark the page that has updates and patches for that software. You'll want to check these sites regularly and always keep your software up-to-date with the latest patches. Some companies even have services that will email you whenever there's a new update or patch.

Security Expert Web Sites

In addition to staying on top of your vendors' security updates and patches, you should also stay current on the security risks and problems that are identified by security experts in the industry. Often, vulnerabilities may become known long before a vendor issues a patch. Therefore, your systems could be vulnerable for a period during which the hackers may know about it, but you don't. Two Web sites that will keep you informed are *http://www.atstake.com/* and *http://www.403-security.org*.

THE PROBLEMS OF THE PRESENT

An IT worker faced federal criminal charges recently in U.S. District Court in Miami for allegedly downloading a virus into his employer's computer system, crashing the network for nearly two full days. This case, which comes a little more than a year after the first federal criminal prosecution of computer sabotage, is just one in a growing number of insider-based network attacks, according to federal law enforcement agents. Another case is getting ready to go to trial in Las Vegas, and yet another was wrapped up with a guilty verdict in New Hampshire (see sidebar, "Insider Accounts").

INSIDER ACCOUNTS

It's a scary indicator of a spiraling economy that in 2004, 7.7 million workers were laid off according to the U.S Department of Labor. Even scarier is the question of how many of those workers still have active accounts on the networks of their former employers. So-called ghost accounts, those not closed when workers leave, can include access to mainframes, databases, file servers, intranets, and email. There are also remote access holes with virtual private network (VPN) passwords and dial-in accounts. All open back doors into a network.

A recent series of high-profile network sabotage cases show that vengeful employees can wreak high-tech havoc. Disgruntled employees are a significant threat. Security experts recommend a combination of procedures, policies, and automation to combat the threat.

Automation is key and is being made available in a class of products known as provisioning software, which can automatically activate and deactivate user accounts. If you are a chief information officer (CIO) and are currently using a manual process, fundamentally you have no way to know if the process of deprovisioning worked. With provisioning software, you know that the process was completed.

However, the process must include social engineering. That means teaching employees not to share passwords and administrators not to reactivate closed accounts. For example, there was one case where a former Coast Guard employee was able to hack into a database using a password given to her by an unsuspecting coworker. The result: A bill of $80,000 and 5,200 staff hours to repair the damage.

The U.S. Secret Service, which splits its focus between protecting heads of state and conducting criminal investigations, is handling twice as many cases that involve insider attacks than occurred in 2004. The FBI is currently investigating seven such cases in New England alone.

Eighty-three percent of the cases are from the inside or people who were formerly with an organization. When you conduct an investigation, that's one of the first areas you need to look at now. It's not at matter of if you're going to be attacked, but when you're going to be attacked. Of the eighty-three percent of the insider cases mentioned in the preceding, ninety-five percent of those break-ins are handled by these agencies. An insider attack really gets the attention of the company, because an insider has access to all the critical systems. If they want to do damage, they know how. A company's decision to protect itself isn't just a technology decision. It's a business decision.

Grocer Victimized

In the Miami case previously mentioned, Herbert Pierre-Louis, a hardware engineer who worked in the IT department at Purity Wholesale Grocers, is being charged with computer sabotage for the June 18, 1998, incident at the $2.6 billion national grocery outlet based in Boca Raton, Florida. The Assistant U.S. Attorney indicated the damage was well over the $6,000 waterline that is one of the key factors making this a federal crime.

The FBI warns that this is a time when companies should be particularly cautious. In light of the economy and the downturn and layoffs, companies should pay attention to this. These are not isolated events.

That's a lesson Omega Engineering's Bridgeport, New Jersey, manufacturing plant learned the hard way. In the summer of 1997, a software timebomb went off in the plant's computer network, systematically eradicating all the programs that ran the company's manufacturing operations. Exacerbating the problem, Omega's only backup tape was missing. The manufacturing plant was no longer able to manufacture. Company executives, in a 2001 trial in U.S. District Court in Newark, New Jersey, indicated that the company had yet to fully recover. The incident caused $23 million in damages and led to Omega losing its footing in the high-tech instrument and measurement market and the eventual layoff of 90 employees.

Omega's former network administrator was charged with sabotaging the network he helped build. He was found guilty after a four-week trial. The judge later set that verdict aside after a juror told the court she was unsure whether a piece of information she had heard on television news had been factored into her verdict. The government appealed the judge's ruling, taking its case in front of the Third Circuit Court of Appeals in Philadelphia this past April. A ruling is pending.

The employee was charged under a relatively new statute that made computer sabotage a federal offense if it affected a computer used in interstate commerce and caused more than $5,000 worth of damage to the company over a 12-month span. That was the first federal criminal prosecution of computer sabotage.

Similar Cases Prosecuted

Now that same statute is being used in three other cases. One of those cases charges a network consultant with sabotaging the computer network at one of his clients, Steinberg Diagnostic Medical Imaging in Las Vegas. The consultant is charged with three counts of network intrusion for changing passwords in the network, which locked administrators out of their own system. The Assistant U.S. Attorney notes in the indictment that the consultant allegedly hacked the system on three different days between late February and early March of 2001.

The consultant, working with a partner, had been hired as a subcontractor by the medical imaging company, according to sources close to the investigation. Both the deal and the partnership fell through, and the consultant's partner went to work for Steinberg Diagnostic as a system administrator. The government contends that the consultant attacked the system to gain revenge. The damage had to have added up to at least $5,000 for the consultant to be charged with a federal offense.

In the summer of 2001, a former help desk worker at Bricsnet, a Portsmouth, New Hampshire, application service provider for the construction and design industry, was found guilty on federal charges of network sabotage for hacking into Bricsnet's system after being fired in the fall of 2000. The worker pleaded guilty to breaking into the system twice using a supervisor's password (once the night he was fired and again the next morning) to delete a total of 786 files, change user access levels, and send emails to Bricsnet clients saying the company's project center would be temporarily or permanently shut down. The attack, which was discovered by another Bricsnet employee the next day, cost the company $24,725 in in-house repair costs. Some of the destroyed files could not be restored.

The fired worker's activities were meant to cause as much damage as possible. It was malicious. Putting a financial number on the loss is misleading. How do you quantify the impact when customers receive these kind of damaging emails? You can't put a dollar amount on that. Would a company pay $24,000 not to have that happen?

Administrators took basic security precautions after firing the worker, who had broken company rules against moonlighting and other activities. They terminated the worker's password, logon, and user accounts. They also changed the code on their building's keypad and escorted the worker from the building. There was no sense of foreboding. These steps were routine. Certainly, Bricsnet had an extensive security system in place, but they were always thinking of outside intrusion.

The incident, which the FBI traced back to the worker in less than a week, has changed the way the company evaluates its security needs. Since the attack, Bricsnet has re-evaluated its security system and limited network access. Bricsnet is acutely aware of the damage a disgruntled employee can cause. People took it personally. For someone you've worked with on a daily basis, it certainly was an act of betrayal for them.

Outlook for the Future

Atlanta-based Internet Security Systems Inc. (ISS) has long been concerned about drive-by hackers. That's right—drive-by hackers. ISS claims perpetrators can equip their laptops with wireless technology [6], sit inconspicuously on a park bench or in a car, and casually monitor traffic, access applications, and hijack data flowing over someone else's wireless network, unbeknownst to the victim. To combat this threat, which sounds like it could be a plot line from an upcoming James Bond film, ISS recently drew the curtain on wireless local area network (WLAN) security software and consulting practices.

Why create safety for the WLAN? ISS believes enterprises are deploying WLANs with increasing regularity because they are cost-effective and help workers grab knowledge on the go from laptops or personal digital assistants (PDAs). Very little exists in the way of security for wireless networks as compared to their wired counterparts, LANs.

Gartner Group, it would seem, concurs that wireless networks are in the midst of proliferation. The research firm said 90% of all enterprises in the United States will have deployed a WLAN by 2006, an increase from 50% in 2003. Accordingly, ISS indicates that the fact that WLANs can easily be accessed by outsiders (friendly or not), means that they need stronger protection.

Just as perpetrators such as hackers and crackers have done to wired networks, they can assault WLANs through the same methods: unauthorized access points, data interception, DoS attacks, peer-to-peer sabotage, and wireless laptops to attacks when they roam to public access points such as airports and hotels.

What is more frightening, ISS claims, is that nontechnical employees, although often victims of attacks, are often unaware of these threats. This ignorance can make the comfort of the firewall a false security blanket.

Most companies have no idea that their networks are wide open to wireless security risks. Employees today are adding their own wireless access points to the backbone of their company's network without the knowledge of their IT and security staffs. With a lack of awareness by the company that an access point has been added and a lack of proper security configuration, these rogue access points can become an intruder's dream back door into a company's network despite the front door firewall.

SUMMARY

This chapter introduced numerous solutions to those of you who are in the process of conducting advanced computer forensics through the use of encryption for protection and hacking back with advanced hacker trackers. Hackers and crackers are everywhere, but you may think your company's system is too minor for them to notice. Not true. Hackers don't always target specific machines—they scan hundreds with special programs to find any that might be vulnerable to attack. The intruder could be a teen hoping to use your system to launch an attack on a Web site, or a bitter ex-employee looking for payback.

The Internet today is like a walk through a vineyard, with the attackers stopping here and there to pick a grape at their leisure. The feast is seemingly never-ending. Even a secure company network can be riddled with holes such as badly configured routers that expose data in transit to snoops. Think your firewall will protect you? Not always. Attacks at Microsoft and EBay prove otherwise.

Furthermore, protecting your network against hackers need not be a full-time job. By including a few best practices as part of your organization's daily routine, you can prevent leaks from developing—or at the very least, plug them before the dams break altogether.

Computer forensics provides the methodology for investigating and documenting cyber crimes so they may be later tried in court. Hiring an expert is costly but necessary to preserve evidence during the legal process.

Also, tools for sifting digital media and detecting network intrusion have become easier to implement, but they still demand a sizeable time commitment and cross-discipline knowledge for most situations. Training is required to secure a crime scene and for procedural litigation.

Conclusions

- Hackers often break into computers through well-documented holes (they read security alerts, too) when users don't install patches.
- Hackers often enter networks through old computers that are no longer in use. This can happen when administrators forget to disconnect an ex-employee's system from the modem or network.
- An older system is less likely to have the latest security patches installed.
- A shared terminal that's not attached to any one employee is often overlooked when security updates are done.
- Any workstation that's left on and connected to both a modem and the network gives hackers one way to dial into the machine, bypass the firewall, and gain access to the network.
- You encrypt important data on your server, but you neglect to encrypt remote backups.
- Hackers can target data on a less-protected off-site machine that stores backups.
- Security is an ongoing task. It's not something you install and forget about; it's something you live with.
- Intrusion detection systems (IDSs) come in several forms, with the most commonly deployed called "host" and "network" systems. Some experts include the

"desktop" IDS in this market, whereas others would also list so-called honeypots and honeynets.

- A host-based IDS is a piece of software that runs on a network-based computer—a Web or application server, for instance. It tracks and analyzes entries in the host system's application and operating system event logs.
- Host-based systems are particularly valuable in monitoring insider threats because they can show when unauthorized personnel attempt to access prohibited data or resources.
- A network-based IDS, which can be software running on a stand-alone PC or on a dedicated appliance, tracks and analyzes the packets that make up network data traffic.
- Network-based IDSs are generally "promiscuous" in that they look at every packet on a network or network segment.
- Network-node IDS systems detect packets headed to a single network node.
- A desktop IDS offers file-level protection. Rather than monitoring network traffic, it examines activity on individual systems, looking for potential attacks on files or registry entries on Windows PCs.
- The desktop IDS is also very useful in trojan horse detection.
- A honeypot is a system designed to be attacked, with the intent of deception or alerting of intrusion activity.
- Honeypots emulate known vulnerabilities, other systems, or are modified production systems that create "caged" environments.
- A honeynet is a network of production systems, residing behind a firewall, which is designed to be compromised. Once breached, the resulting information gathered during the attack is analyzed to learn about the tools, tactics, and motives of the possible intrusion.

An Agenda for Action

Table F20.1 in Appendix F is a provisional list of actions for advanced computer forensics. The order is not significant; however, these are the activities for which the researcher would want to provide a detailed description of procedures, review, and assessment for ease of use and admissibility. A number of these advanced computer forensics topics have been mentioned in passing already.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises, hands-on projects, case projects, and optional team case project. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? Hackers often break into computers through well-documented holes (they read security alerts, too) when users install patches.
2. True or False? Hackers often enter networks through old computers that are no longer in use. This can happen when administrators forget to disconnect an ex-employee's system from the modem or network.
3. True or False? Host-based systems are particularly valuable in monitoring outsider threats because they can show when unauthorized personnel attempt to access prohibited data or resources.
4. True or False? A network-based IDS, which can be software running on multiple PCs or on a dedicated appliance, tracks and analyzes the packets that make up network data traffic.
5. True or False? Honeypots emulate unknown vulnerabilities, other systems, or are modified production systems that create "caged" environments.

Multiple Choice

1. Because the Internet is built upon the TCP/IP protocol, many hacker attacks will seek to exploit the TCP ports of these servers with public IP addresses. A number of common ports are scanned and attacked, except:

   A. FTP (21)
   B. Telnet (23)
   C. SMTP (25)
   D. INS (53)
   E. HTTP (80)

2. Private citizens have legitimate reasons to do the following, except:

   A. Preserve confidentiality
   B. Protect flaws
   C. Protect trade secrets
   D. Prevent legal or medical records from falling into strangers' hands
   E. Voice dissenting political or religious opinions without retribution

3. You only have three directions to go with hacking, except:

   A. You can keep doing the same old tricks.
   B. You can become a real criminal cracker.

C. You can be hired to hack other hackers.
D. You can use those skills wisely to build new software and create a more secure Internet.

4. Just as perpetrators such as hackers and crackers have done to wired networks, they can assault WLANs through the same methods, except:

A. Unauthorized access points
B. Data interception
C. Denial-of-service (DoS) attacks
D. Authorized access points
E. Peer-to-peer sabotage

5. Hackers can do the following, except:

A. Break into computers through well-documented holes (they read security alerts, too) when users don't install patches.
B. Enter networks through old computers that are no longer in use. This can happen when administrators forget to disconnect an ex-employee's system from the modem or network.
C. Target data on a less-protected off-site machine that stores backups.
D. Dial into the machine, bypass the firewall, and gain access to the network.
E. Physically destroy a network.

Exercise

A large financial institution routinely used a computer forensics specialist team (CFST) to investigate corporate computer-usage policy violations. The CFST is used as part of the process to discreetly investigate and verify allegations of computer-usage policy violations, performance issues, and other policy violations. So, how was the CFST able to go about conducting their investigations?

HANDS-ON PROJECTS

A large insurance company used a CFST for incident response activities and deployed the CFST on 36,000 machines within their organization. How was the CFST able to go about conducting their investigations?

Case Project

A large telecommunications company uses a CFS to protect against potential litigation from wrongful termination lawsuits and other employee accusations. Organizations face many challenges and potential repercussions when terminating employees. This organization uses a CFS to proactively acquire forensic hard drive images of employees' computers prior to termination. How did the CFS go about conducting the investigation?

Optional Team Case Project

A large insurance institution uses a CFS to investigate suspicious insurance claims and to determine if there is employee collaboration in fraudulent claims. How was the CFS able to go about conducting the investigation?

REFERENCES

[1] Vacca, John R., *Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan*, McGraw-Hill, New York, 2001.

[2] Caloyannides, Michael A., "Encryption Wars: Early Battles" (© 2000 IEEE), IEEE Spectrum, 445 Hoes Lane, Piscataway, New Jersey 08855, 2001.

[3] Vacca, John R., *i-mode Crash Course*, McGraw-Hill, New York, 2002.

[4] Vacca, John R., *Electronic Commerce*, 3rd ed., Charles River Media, Hingham, MA, 2001.

[5] Vacca, John R., *High-Speed Cisco Networks: Planning, Design, and Implementation*, CRC Press, Boca Raton, FL, 2002.

[6] Vacca, John R., *Wireless Broadband Networks Handbook*, McGraw-Hill, New York, 2001.

This page intentionally left blank

21 Summary, Conclusions, and Recommendations

Computer forensics may sound like a media-generated catchphrase, but its principle is actually quite simple. Forensics, generally speaking, is the investigation of evidence following scientific methods within the regulations of the law. Computer forensics applies those same principles to digital evidence recovery.

The scope of such digital-evidence salvage operations is enormous because of many factors, including the global nature of the Internet. To help create cooperation between the United States and other nations, the G8 group (*http://www.g8online.org/*) of major industrialized nations has proposed six principles for procedures relating to digital evidence, which it defines as *information stored or transmitted in binary form that may be relied on in court*:

1. When dealing with digital evidence, all the standard forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. People who access original digital evidence should be trained for the purpose.
4. All activity relating to the seizure, access, storage [1], or transfer of digital evidence must be fully documented, preserved, and available for review.
5. Individuals are responsible for all actions taken with respect to digital evidence while such evidence is in their possession.
6. Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for complying with these principles [2].

All computer forensic policy and procedures should be developed from these principles. Not limited to computers in the traditional sense, the field encompasses everything from personal digital assistants (PDAs) to routers and covers crimes ranging from creating, possessing, and disseminating child pornography to network intrusions. Perpetrators range from 13-year-olds to trained experts paid by rogue nations to infiltrate and steal proprietary information; organization insiders could also perpetrate similar crimes.

SUMMARY

The United States Department of Justice categorizes computers involved in crimes in three ways: contraband, instrumentality, and "mere" evidence. If a network manager discovers contraband (illegal or illegally acquired equipment), he or she should simply turn the matter over to law enforcement.

Computer instrumentality implies that hardware played a significant role in a crime. Within network-related crimes, "innocent" computers are often used as instrumentalities—they are used to commit further crime, either denial of service attacks or by providing a pass through for the criminal. Law enforcement will often seize computers used as instrumentalities; they must seize them if the crime falls under certain federal statutes.

Computers classified as mere evidence are usually not seized. The goal is to acquire the data of evidentiary value from the computer while adhering to computer forensic principles. Before getting into specifics on how this is done, let us first examine some policies that should be in place before the need for forensics arises.

Haste Makes Waste

Every business should have a computer security plan, part of which must include collection and preservation of evidence before, during, and after the incident. When formulating all policies regarding computer forensics, a balance must be struck between expediency and following a proper chain of command. It is neither feasible nor desirable for the chief information officer (CIO) of a large corporation to be called every time a computer is attacked; at the same time, some oversight is important. Each organization needs to decide how far to proceed up the hierarchy when responding to different levels of attacks.

Because laws will affect corporations differently, and because desktop forensics is extremely important for internal offenses, it is wise to have separate policies for internal attacks and external attacks. A recent study performed jointly by the Computer Securities Institute (CSI) and the National Infrastructure Protection Center arm of the FBI found that a significant number of attacks (84%) came from disgruntled employees. This is not only the case at university-type settings, where public labs are plentiful and security is often lax, but remains true for all types of organizations.

When dealing with internal policies, desktop examination is a crucial element, whether the matter is simple misuse or corporate espionage. Regardless of the reasons, following proper forensic procedures will help establish a legal case.

NOTE *Certain laws exist to provide some privacy to the end user [3].*

The one most important privacy law for this chapter and book is the Electronic Communication Privacy Act (ECPA), which begins in the United States Code at Title 18, section 2701. The law contains certain provisions that should be incorporated into every policy. For the purposes of this chapter, assume you are dealing with an email system that employs user authentication to verify active employee status. Policy rules regarding an open Internet service provider (wherein anyone can pay and join) are significantly more stringent.

NOTE *One provision of the law, Title 18 USC 2703(f), applies equally to all email providers: "A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."*

Law enforcement commonly refers to Title 18 USC 2703(f) as sending an "F-letter" (referencing that the law is section F of the statute) to a provider. Usually such a request will be communicated via telephone first, followed by a letter. A company should immediately take the steps mandated via the phone call, without waiting for the letter's arrival. Under the second part of this section, the records must be preserved for 90 days, and the government has an option to extend this another 90 days. There should be appropriate policies in place to handle this possibility, from the administrative receiving end all the way to placement of the backed-up records. These policies should be created in a partnership among management, computer services personnel, and legal counsel.

How does a manager know if the staff possesses the requisite knowledge to create sound corporate policies on evidence recovery? This is an extremely difficult question to answer, but one approach might be to determine who, typically, would not be qualified. The average system administrator usually doesn't have the required knowledge; the Microsoft-certified systems engineer (MCSE) test also doesn't have such information. A dedicated network security specialist may or may not have the appropriate knowledge, but this is probably the best place to start looking. That individual, who might be a certified information systems security professional (CISSP) or System Administration, Networking, and Security Institute (SANS) certified, will have a fundamental understanding of security issues that a normal system administrator probably would not.

Mapping the Labyrinth

Even though the corporate computer forensics specialist is not a law enforcement officer, he or she will still find merit in following the same forensic procedures. This includes limiting access, photographing the computer screen if information is visible, and, most important, documenting every step. From the moment a computer is recognized as compromised, documenting should begin.

Documentation should hold to a general standard: If someone with comparable knowledge picks up the first examiner's notes, he or she should be able to reach the same conclusion after following each step. Documentation should include the basic "who, what, when, and where" criteria and how long each individual spent diagnosing and repairing any problems, which is used to determine damages. The amount of damage may not only influence the involvement of federal investigators but also a resulting federal trial; under U.S. Federal Sentencing Guidelines, damages determine the punishment.

It is essential for companies to keep track of their damages when responding to an intrusion threat for purposes of criminal prosecution. The costs incurred by a company to detect, repair, and deter future intrusions, including labor costs, are used by the courts in determining the sentence for an intruder. Thus, companies are asked to keep track of their costs so that intruders can be effectively prosecuted.

NOTE

For laptops or machines with an internal, uninterruptible power supply, disconnect the internal ups or battery before the power cord is pulled. Afterward, the hard drive is usually removed and reinstalled on another machine. The system is booted from a floppy that disallows any attempt to write to the hard drive, and a bitstream image is created via one of a variety of products.

What imaging software you choose to use is largely a personal preference, provided that it satisfies the criterion of providing complete bit-by-bit imaging. The person performing the imaging procedure must verify the software's ability and accuracy every time a new update is released. Some popular choices (although this author and publisher are not endorsing any) are Safeback (*http://www.forensics-intl.com/safeback.html*), Fred (*http://www.digitalintel.com/*), and Encase (*http://www.encase.com/html/index.html*).

Some popular commercial imaging software may or may not offer forensic capabilities. It may be an option. Just remember that before any software is used, the individual performing the image must verify it. This is done by proper hash testing, discussed later on.

Sealing Off the Unix Crime Scene

Unix can be more problematic in response to a forced shutdown that occurs because of power loss. There are several options and opinions within the field regarding how best to handle a Unix box. How the shutdown should be handled will depend on how critical the data on the victimized computer is, among other criteria. Regardless, the first step is, as always, to document the state of the system before touching it. This may include photographing the monitor and the computer. The next step is to collect any possible evidence from RAM, accomplished by using the command line "ps -aux" or "ps -ef," depending on the Unix version.

The individual should look for and be able to recognize any programs that are unauthorized. If any are found, the associated RAM contents should be saved. The method for accomplishing this may vary with the Unix version, but one example is the "gcore" command. A computer forensics specialist should also be familiar with programs such as List Open Files, beneficial in isolating trouble spots. It's important to make sure all programs are authentic and updated; intruders may replace commands with their own "trapped" versions.

After RAM documentation, there are several options: one is to sync, halt, reboot, and mount the drives from a CD. One possible danger is that the sync command may have been altered, thus damaging evidence. This procedure also changes the state of the hard drive, which is a possible concern. Another option is simply to pull the power and leave the system in a dirty state. Afterward, the drive can be mounted dirty, and bit-stream copies can be created from the original.

A third option is to make a bit-stream copy by utilizing the Data Definition "dd" command. This is not a command that can be covered briefly, as it has many options and parameters, such as identifying a data-definition element in a definition list and converting a file while copying it. It is important that any person using this command is trained to do so.

Truth Serum

No matter what operating system (or program used to create copies) is being utilized, some type of verification software should be part of the forensics equation. The purpose of these programs is to ensure that the copy of the bit-stream image of the violated computer is the same as the original. This is accomplished by using mathematical algorithms, called "hash functions," which calculate hash values (also known as checksums, or fingerprints) based on the original file or image. To be valid, hash functions must meet two primary requirements: The original text may not be determined from the hash function, and they must be collision free—meaning that two different messages cannot produce the same hash value.

A file-hashing utility should always be used to verify the copying of all files or images. The use of the SHA-1 hash is highly recommend. The hash values should be recorded and kept in order, along with such data as when the program was run, who ran it, and what program was used—valuable information for the event reconstruction typical of court cases.

Security Officer's Log: Mission-Critical

Logs create evidence when they capture the actions of an illegal act. What logs an organization chooses to keep, and how long it will keep them, largely depends on available space and average number of entries received. It might see frequent probes—anything from port scans to domain name service (DNS)-version requests on an open system. Although such probes are annoyances that are not even necessarily illegal, it may be important to keep logs of them. If the organization chooses to go to court, such logs will provide a complete picture for a jury.

To keep logs from being destroyed by malicious intrusions, system operators will often output some logs to a printer or a CD-ROM device; this can be an expensive route, but it frequently offers greater security. If utilized, this option should be noted in an organization's policies and procedures, as law enforcement may not automatically think to ask for logs copied in this fashion.

NOTE

Different versions of Unix have their logs in different areas. Most of the older versions keep logs in /usr/adm, whereas most newer versions use /var/adm or /var/log for storage.

One of the primary logs used in computer forensics is syslog, the main system log containing a variety of important messages. This is no secret to hackers, and hence is often one of the first logs to be modified. In addition, routers and firewalls can be configured to add messages to the syslog.

NOTE

A high degree of redundancy exists between syslog's contents and other logs, so they should be checked against each other; log inconsistencies may indicate security breaches.

Some popular logs that may prove useful include acct, aculog, lastlog, loginlog, sulog, utmp(x), wtmp(x), void.log, and xferlog. Remember that when any of these logs are copied, a hashing program should be used to ensure proper backup creation.

Windows NT's three main log files—appevent.evt, secevent.evt, and sysevent.evt—are kept in the percentsystemroot percent\system32\config directory and are normally viewed using Microsoft's built-in Event Viewer. Various Web and ftp servers will also have their own logs and should be preserved as well. It is important to have a current list of programs and services installed and to have a checklist for log preservation.

Ghosts from the Immediate Past

State tables are another potentially important source of evidence, although their temporary nature makes them difficult to acquire. State tables show actions that take place either in real time or in the immediate past. One of the most popular and powerful is the Netstat command, which exists in both Unix and Windows NT environments, with different options for each. The Netstat command displays network connections, routing tables, interface statistics, masquerade connections, netlink messages, and multicast memberships.

Another temporary log that can sometimes be useful is a system's address resolution protocol (ARP) cache, designed to discover media access control (MAC) addresses on Ethernet-based networks. MAC addresses do not cross routers. This is important because packets sent over the Internet will not contain the sender's MAC address, but instead, will have the MAC address of the last router they traversed. If the router is keeping the correct logs, and a packet has only traveled over a few routers, this information may be useful. Both NT and Unix create a temporary cache list of the IP-to-MAC conversions, viewable by using the Arp-a command.

There are special steps for state table preservation. Not only should they be cut and pasted to a text file, but printing the screen shot is also advisable. The log should then be hashed and preserved with other evidence.

Protecting the Evidence

Generally speaking, two separate backups of every relevant file and image should be made. These files should be hashed along with the original. The media a company chooses to use will depend on size, speed, and cost issues (tapes versus DVD-RAM versus identical hard disk drives, and so on). More important still is the method by which those media are handled. The forensic chain of evidence requires that the person creating the backups, along with anyone who touches the media prior to presentation in court, be clearly documented. Obviously, care must also be taken to protect the media from various environmental elements: preferably, it should be placed in an appropriate container, taped shut, then initialed and dated. This ensures media authenticity after completion of the backup. Some type of standard tracking method should be used with every piece of evidence.

Costs of Precaution

No summary chapter on computer forensics would be complete without an examination of costs involved. There are two types of costs: the cost of doing nothing about data-evidence recovery and the cost of doing something about it. The most recent CSI/FBI study reported that total losses incurred via data loss, fraud, or abuse for 506 respondents totaled $598,812,273.

Personnel costs associated with computer forensics are dependent on several factors, including the number of different operating systems the person is expected to know. Each additional operating system requires additional training. Costs are fluid and should be taken only as ballpark figures. Training a staffer with preexisting knowledge to be the rough equivalent of an individual in a forensic laboratory may cost around $58,000 for one platform. Costs for materials examination may run from $40 to $700 for one case. The salary level of the examiner will fluctuate with location and experience. It is possible, of course, to hire an outside forensics specialist. The cost for this type of service varies greatly.

There is a wide range of options when it comes to the software. The cost of forensic tools may range from no cost for older, basic tools to over $4,800 for one software package alone. There are also costs for password cracking, both for software and the time necessary on a computer (cost per CPU cycle). It is important to reiterate that every company should keep track of all costs related to the attack, including the amount of time each person spends responding to any damage. Tracking all of these costs is extremely helpful if any court proceedings occur.

Homegrown Salvage Team

Computer forensics is an important part of a larger picture. Every organization should consider forming a computer security incident response team (CSIRT, sometimes referred to as a Computer Emergency Response Team, or CERT), if one hasn't already been established.

Incorporating computer forensics into the responsibilities of any CSIRT bolsters organizational security and makes court actions more successful. This can help create a safer environment for an organization's employees, customers, and business partners.

Computer Forensics to Play Central Role in Terrorist Fight

Computer forensics begins at home. For the IT manager, that means the server room, where the Internet has brought not only the promise of a worldwide audience but also the threat of worms, hackers, and cyberterrorism. As the United States mobilizes to shore up security at airports and public gathering spaces and in the country's infrastructure, the IT industry has a central role to play—a role that not only makes business sense but also is important in the unfolding war on terror.

In the same week that the terrorist destruction of the World Trade Center took place, the Nimda worm ran rampant through the Internet. Although there may not be any overt connection between the two events, the continued marauding of worms and viruses across the Net only reinforces a general anxiety about living in an insecure world and a specific feeling that the Net will never be a place where real business can be conducted.

Much of enterprise IT security has been built around firewalls or monitoring products meant to keep the bad guys out. Although that is fine for providing a sense of relief that you avoided the virus that halted the company down the hall, it doesn't do much to solve the problem.

The role of computer forensics in the current rush to security cannot be overstated. Before the government rushes to mandate face scanners, fingerprint identification systems, or simply networks to signal when a bad guy might be applying for a crop duster license, there has to be some consideration of the systems that will be required to run these programs. Developing systems that have what appears to be an effective front end, but in reality are porous, is at least partly to blame for the lax airport security programs that had such a horrific result and still do.

Scanning in lots of data, tapping lots of phones, or opening lots of encrypted email can drown you in data if you don't have some way to collect, sort, and analyze it and alert the security official who needs to know of a breach in process. Too much data is often more dangerous than too little, as overwhelming data can give you a false sense of security.

Where does that system expertise reside? It resides in systems that manage credit-card transactions, in phone connection and billing systems, and in data-management systems. The war on terror will be marked by huge amounts of data, gathered electronically and in person, that will be analyzed to focus on a small group of fanatics. It is telling that President Bush used an attack on financial information as the first salvo in the terror war. The IT sector through computer forensics has a crucial role to play in stopping the terrorists before they can strike again.

CONCLUSIONS

The federal government can report in exacting detail the number of bank robberies committed in any given year, but when it comes to computer crimes against government agencies, it's close to clueless. Government officials estimate that only 20% of such incidents are reported because individual agencies either don't have the technical sophistication to discover the crimes or want to keep bad news quiet. It's for those reasons that the 599 root compromises of federal computers reported in 2004 likely represent a fraction of the actual number.

Computer compromises are a serious issue. Agencies fear the unwelcome attention computer crime reports bring and often lack the money and tools needed to detect IT security breaches. In addition, there's an ingrained reluctance on the part of agencies to work together to combat computer crimes. There is no culture of collaboration in the federal government.

During the first three months of 2004, the Federal Computer Incident Response Center (FedCIRC), the government's central crime data repository, recorded 88 root compromises at civilian nondefense federal agencies, which put it on pace to exceed the 2003 total. That would result in an increase in the number of such intrusions for the third straight year.

A root compromise occurs when an intruder gains systems administration privileges on a network, giving the attacker the ability to do things such as copy documents, alter data, or plant malicious code. Still, security analysts said it's impossible to gauge just what the first-quarter increase recorded by FedCIRC (*http://www.us-cert.gov/federal/*) means. FedCIRC doesn't know whether they're seeing a change in the rate of reporting, the rate of detection, or the rate of penetration.

For its part (prior to the 9-11 attacks), the Bush administration had begun to take steps to improve compliance by federal agencies in reporting and responding to security breaches, including a recommendation that FedCIRC's annual funding be boosted 27%, from $11 million to $14 million. Agencies are already required by law to report breaches to FedCIRC as a result of the Government Security Reform Act approved in 2000.

Federal agencies have repeatedly been faulted by the General Accounting Office (GAO) for poor security practices. The 9-11 attacks and the recent issuance of educational visas to the dead terrorists have borne that out. The GAO has conducted penetration testing against various government systems. For example, it said in a report recently released that it found significant security weaknesses at all of the 24 agencies where it conducted audits of IT security readiness. Improving security procedures needs to be a priority within the Bush administration, and from some of the early indications in the budget, it is going to be.

Cost of Computer Crime Exploding

According to results of the 2004 Computer Crime and Security Survey [3a] recently released, intellectual property theft and security breaches are on the rise and the costs of those intrusions are skyrocketing. Conducted by the Computer Security Institute of San Francisco and the FBI, the survey of 972 security administrators from industry, government, and academia shows that 89% of respondents reported security breaches in the 2004 survey and 30% reported intellectual property theft, up from 24% in 2003.

The survey also shows that the cost of that theft is exploding. Although only 68 respondents could quantify the financial losses associated with intellectual property theft, that number added up to more than $595 million. The amount is up from almost $101 million in 2003 and $64 million in 2000. In total, 520 respondents said losses from all types of security breaches cost more than $711 million. That means theft of intellectual property accounts for 44% of all losses tabulated in the survey, despite the fact that such a small number of companies could quantify it.

Companies are figuring out how to protect their financial data, customers' credit information, and personnel records. The problem is that many companies aren't aware that they should be protecting the information that fuels their businesses—such as marketing plans, source codes, and research information. You lock up rooms so people can't steal laptops, but if your company is based on information and information systems that can't be secured, then you're in line to lose your cash crop.

Industrial espionage is giving way to information age espionage. It used to be that if you wanted information on your competition, you would turn to an insider. You bribed them. You blackmailed them. But why risk someone getting caught when you can just hack in and take what you need? The survey also points to several other aspects of computer security that are on the rise:

- Forty-four percent of respondents reported outside system penetration. That number is up from 24% in 2001.
- Forty-two percent detected denial-of-service attacks. That number is up from 28% in 2002 and 31% in 2003.
- In 2004, 683 people were able (and willing) to quantify financial losses. That number totaled $609 million.
- Forty percent of respondents reported security breaches to law enforcement agencies. That's up from 21% in 2001 and 29% in 2003.

Industry analysts and corporate users agree that more administrators should be focused on protecting their valuable proprietary information. Companies that collect credit card numbers and personal information about people take on that security responsibility. What they're not doing is protecting their own information, records, plans, and technologies.

For some IT administrators, getting the message through to upper management is another matter. It's not that upper management doubts the information's value, but rather that upper management feels that there isn't enough threat to warrant any significant attention. Once management buys into the importance of protecting information, it's another matter to put a strong security plan in place.

Companies developing a new drug or a new widget may understand how sensitive that product information is, but they find it hard to protect. It's the core of what they're doing, so it requires access from a lot of people for a lot of reasons. It's difficult to enforce protection of information while still letting people at the information.

The survey trends are unnerving. It's clearly a dangerous world, and will continue so for years to come—possibly even get worse—given the widespread deployment of computer forensics and security technologies. It's costing American businesses billions.

RECOMMENDATIONS

Details of the arrest of U.S. Federal Bureau of Investigation Special Agent Robert P. Hanssen for espionage highlight the need for increasingly sophisticated computer forensic imaging and analysis tools and methodologies for their proper use. The FBI conducted a search of Mr. Hanssen's briefcase in 2001 and found a "computer memory card," from which they were able to retrieve a digital copy of a note Mr. Hanssen wrote to his Russian handlers in 2000. The digital copy was made in the off-limits room Hanssen kept in his basement—the one with two computers that authorities believe he used to maintain his own spy operation.

Few of us will ever be in as tense a situation as the one the FBI faced recently with Mr. Hanssen and the "computer memory card" or the off-limits room in the basement. Mess that up from an evidence-handling perspective and a major international espionage case could evaporate, but no matter where you work in the computer security field, you may one day find yourself faced with a tough investigative challenge—looking for the right tools to accomplish an incredibly important job, facing near impossible deadlines—and always with the thought in the back of your mind that if you mess something up, life as you know it could change drastically.

The need for technical investigative capabilities has been growing steadily with the proliferation of computers in the workplace, and the discipline of computer forensics has emerged to meet that need. Computers being what they are, it takes a computer and a robust set of applications to analyze another computer in such a manner that the results of the analysis are thorough, sound, unbiased, and repeatable. That's where the various developers and vendors of computer forensic analysis software come in. Each developer has his or her own unique perspective on the needs of the investigative community and his or her own approach as to how to meet those needs, but few have started the software-development process with a well-stated computer forensic analysis requirements document.

What tasks must computer forensic analysis software be able to accomplish? How can you measure the performance of various tools against one another without a well-defined requirements definition? The speed of a forensic analysis tool is of little consequence if it is not also thorough, unbiased, and forensically sound, so speed alone cannot be the primary consideration. The knowledge, skills, and experience of the analyst at the keyboard can also play a significant role in the performance of a tool when no thorough requirements document exists.

This final recommendations section is concerned with how to conduct a relevant and meaningful review of computer-forensic-analysis software tools. Let's start with a requirements definition. With more practitioners involved in stating requirements and designing tests, the tests will be more relevant to the computer forensics community. With luck, where tools fall short of meeting requirements, developers will take the results to their labs and work to improve the tools. It is the intent of this recommendations section to initiate discussion and solidify the various computer forensics requirements.

Requirements Definition

Let's begin this look at requirements by identifying certain capabilities that a forensic examiner needs, based on tasks the examiner must perform to complete a thorough, unbiased, and forensically sound examination of computer media. The requirements definition is not intended to mandate specific procedures or to endorse certain products. It is also not intended to mandate that any specific software tool be used in any specific set of circumstances. Where possible, the requirements definition is also media independent, operating system independent, file system independent, and hardware platform independent.

This requirements definition also takes into account that law enforcement officers have different requirements than corporate security and investigations personnel. Whereas law enforcement officers typically have legal authority to seize computer systems as evidence in criminal cases, corporate security and investigations personnel are typically involved in civil cases and rarely have authority to seize equipment. Corporate security and investigations personnel do typically have some authority to preview systems, determine which ones may have relevant evidence, and preserve evidentiary images of systems deemed to contain relevant evidence. Likewise, where the law enforcement officer may remove evidence to a lab environment for analysis, the corporate security officer will typically remove only evidentiary images of media, leaving the original media on site.

At a fairly fundamental level, the forensic analysis toolbox needs certain capabilities. For instance, you must be able to complete forensically sound searches of computer media at both the logical and physical levels of the media. That requirement exists because certain data in the logical file system may not be readily available or readable at the physical level. As an example, much of the Windows registry is written physically to disk in binary form but is readable logically with a tool such as Regedit.exe. Adobe Acrobat portable document format (.pdf) files are, likewise, physically written to disk in a manner that obscures the textual content of the document. Compressed files, encrypted files, and other "special" files written physically to disk in a format other than text format likewise will not show their real content at the physical level.

A search of computer media at the physical level also might miss plain text words in a document if the document is fragmented physically on disk and the word of interest is partially contained at the end of one sector and the beginning of a noncontiguous sector. Only a logical search of the file system can ensure that relevant text contained in logical files fragmented physically on disk is found, because a logical search can account for fragmentation.

This requirements definition also sets forth minimum requirements for functionality, taking into account a wide variety of technical, logistical, and legal circumstances. The "identify–preserve–analyze–report" model continues to describe the overall process investigators use to conduct an investigation involving computer-based evidence. An investigator at a crime scene must be able to identify computer systems or media possibly containing digital evidence relevant to the case. If a crime scene contains computers, and investigators leave the scene without them (or without forensically sound evidentiary images of them), then the process ends and no analysis or reporting can take place. Any evidence on the media is possibly lost.

Once an investigator identifies the systems or media possibly containing data of an evidentiary nature, he or she must properly preserve their digital contents in a forensically sound manner. After preserving the evidence, an investigator will conduct series of examinations (analyze) of the data on the media to extract relevant information from it. After identifying relevant media, preserving appropriate evidentiary images of the media, and conducting a thorough, unbiased, and forensically sound examination of the media, the investigator will report the results of their efforts in some fashion.

The capabilities an examiner requires for any one step of the process may sometimes overlap with capabilities required for other steps. Essentially, without the capability to do each of these functions, an investigator might not have in his or her toolkit the requisite tools necessary to accomplish a thorough, unbiased examination of media, finding all relevant and potentially incriminating or exculpatory evidence on the media under examination. The following capabilities are useful as a starting point to develop a set of minimum requirements:

- An investigator requires a capability to simultaneously preview a large number of systems on site to determine which ones contain relevant evidence.
- An investigator requires the capability to conduct a search at the physical level of the target media, ignoring operating system and file system logical structures and searching from sector 0 to the end of the media regardless of the logical content.
- The search tool must be able to reliably report the physical location on the media where responsive data were found.
- An investigator requires the capability to conduct a thorough, read-only search at the logical level of the target media.
- An investigator requires an ability to generate a listing of all logical files in a file system.
- An investigator requires an ability to search the contents of the regular files in a file system without changing either the data in the file or any date/time data recorded by the operating system about the file.

- An investigator requires an ability to identify and process special files.
- Investigators require the capability to recover pertinent deleted files or portions thereof that have not been overwritten.
- Investigators require the capability to make forensically sound images of a wide variety of media.
- Investigators require the capability to restore forensic images to suitable media.
- Investigators require the capability to perform a sector-by-sector comparison of two pieces of media to determine where they differ.
- Investigators require the capability to thoroughly document their investigative activities and succinctly document the data recovered from a piece of media that is relevant to the allegations under investigation.

Simultaneously Preview a Large Number of Systems on Site

In some situations, identifying which computers or media at a scene may contain information or data of evidentiary value is fairly straightforward. The hacked Web server, a compromised file server, a firewall, or other networked devices may be, because of the nature of the investigation, an obvious system to preserve. In other cases, particularly where the allegation concerns activities of insiders, it may not be so easy to determine which systems contain information of evidentiary value. In cases where an office has multiple computers, and a subset of those computers might contain relevant evidence, then seizing or imaging all the computers at that site could be a tremendous waste of vital resources.

In most cases, an initial search at the physical level of the media may be sufficient to determine if a specific computer system or piece of media contains relevant information and should be imaged or preserved for further, more detailed analysis. However, keep in mind that a fruitless search at the physical level may have actually missed relevant information for a wide variety of reasons, including that relevant keywords in logical files may be physically fragmented on disk, relevant files may be compressed or encrypted, or relevant files may be otherwise encoded or obscured. The investigator must decide, based on the circumstances of the case, whether a fruitless search at the physical level of the media is sufficient to exclude the media from further processing. Previewing computer media has two subcomponent requirements: a validated read-only methodology and a controlled boot process.

Validated Read-Only Methodology

For previewing media on scene, an investigator requires a capability to preview media using tools and methodologies that have been tested under various circumstances and validated not to make changes to the original media. Otherwise, the preview process itself may taint the evidence by changing pertinent date/time stamps on files or otherwise modifying data on the target media. Unintentionally modifying date/time stamps in particular could unnecessarily complicate the evidence-analysis process.

Controlled Boot Process

For previewing media on scene, an investigator requires a boot process that can be precisely controlled. Whether the preview process will be done via a remote connection to a computer system or will be executed locally on the system, the investigator must know exactly what the boot process is, ensure that the boot process used does not make changes to any of the data on the media to be previewed, and ensure that the preview tools and methodologies are forensically sound.

The preview process itself can be conducted several ways, including either remotely or locally. A local preview of media involves using a controlled boot process to boot the suspect machine and conduct a review of the system locally. If the entire process can be contained on floppy diskette or bootable CD-ROM, this could allow as many simultaneous iterations as there are suspect systems to be previewed, but the local preview process must not make changes to the media being previewed.

Like a local preview, a remote preview must be conducted in such a manner that it does not make changes to the media being previewed. If the investigator uses a tool with a remote preview capability, they will actually boot two computers: the one housing the media to be previewed and the one from which the preview will be accomplished. Using a remote preview capability may limit the number of simultaneous iterations that can be conducted because it requires more hardware, but in cases where only a few systems need to be previewed, a remote capability could be very useful. Typically, remote previewing involves connecting two computers via a parallel port, com port, video port, or other port, running a “server” version of an application on the machine to be previewed, and running a “client” version of the software on the machine from which the preview is conducted. No matter the exact mechanism used, the preview process must be forensically sound and must not make changes to the media being previewed.

Conduct a Search at the Physical Level of the Target Media

A physical search of the media essentially searches all logical files, file slack, free or unallocated space, and all space on the media outside any logical data areas. The search tool must have the ability to use both ASCII and UNICODE character sets. Some operating systems write documents and other files to disk using printable and nonprintable ASCII characters. Other operating systems can use the UNICODE character set as well as the ASCII character set. A search for a word using the ASCII character set will not find that word if it is written to disk using the UNICODE character set, so an investigator requires a search tool that can use both character sets in its searches. Preferably, a single pass through the media will search using both character sets simultaneously.

The search tool must be capable of searching all sectors of the physical media. If the tool cannot see and search all sectors of the media, the resultant search may not be thorough enough to establish that evidence either does or does not reside on the media.

The search tool must be capable of using a keyword list. Tools that require separate passes through the media to search for each keyword would unnecessarily constrain the investigator in terms of both time and efficiency, especially when searching one of today's 80-Gb and larger hard drives. The keyword list must be able to include regular ASCII text as well as hexadecimal notations. Some file type headers and all binary files will contain nonprintable ASCII characters. Hexadecimal notation is the best way to search for this type of data.

Report the Physical Location on the Media

This report could use either the cylinder-head-sector (CHS) or logical block addressing (LBA) address of the responsive data. In the best case, even though a physical search is conducted, the search tool may be able to determine whether the keyword resides in a logical file on the media, file slack, free space, or areas of the media outside the logical data area.

The search tool must be able to show results in context. Rarely is a keyword or phrase so unique to an investigation that its mere presence on a piece of media indicates the media contains data of evidentiary value. The investigator must be able to discern the context within which a word or phrase resides on the media to determine whether the context is relevant to the investigation. Thus, the search tool must be capable of displaying some amount of data that resides on disk immediately prior to the keyword and some amount of data that resides on disk immediately after the keyword. Otherwise, the investigator must use a hex editor to preview each sector containing the key word to determine whether it actually contains relevant data.

An investigator also requires the ability to calculate a hash of the physical media. The hash process must take into account every bit of every byte of every sector on the media, from sector 0 to the last physical sector, regardless of whether any specific sector is included in any logical volume on the media. In most cases, the minimum standard is the 32-bit cyclic redundancy check (CRC) algorithm. For hard drives, the 128-bit message digest 5 (MD5) algorithm is preferred.

Conduct a Thorough Read-Only Search

A search of the logical file space is likely to require less time than a search of the physical media, but likely will not search every sector of the media. If an investigator begins with a logical search to preview media, and that search produces no relevant results, the investigator may have to follow up with a search of the physical media to ensure a thorough search. If the search tool used on one logical partition does not understand the file system formatting of another partition on the media, then a different search tool must be used on the other partition. For instance, a hard drive may be partitioned and formatted to boot multiple operating systems, each using a different file system. That may require several logical level search tools if no one tool understands all the file systems on the media.

As with the physical level search, the search tool must have the ability to use both ASCII and UNICODE character sets. This is for exactly the same reasons as previously stated for searching at the physical level.

The search tool must be capable of searching all sectors within the logical boundaries of the file system. If the tool cannot see and search all sectors of the file system, the resultant search may not be thorough enough to establish that the evidence either does or does not reside on the media. For reasons already stated, the search tool must be able to use a keyword list.

Generate a Listing of All Logical Files

This listing must include not only all the regular files in a file system but also all files with special attributes, such as hidden files, read-only files, system files, executable files, directories, links to files, device files, and so on. The tool that creates this list must be able to write the list of files to appropriate media, whether that is a network-accessible volume, a local hard drive not under investigation, or some appropriate removable media connected to the analysis machine. Preferably, the tool that generates the list of files would not allow the list to be written to the media being searched.

In addition, an investigator requires an ability to generate a listing of all the date/time stamps an operating system may store in relation to each file in the file system. Some operating systems store various dates and times in relation to the files in the file system. Those dates/times may include Date/Time Last Modified, Date/Time Last Accessed, or Date/Time Created. Not all operating systems record all date/time combinations, but if an operating system records any date/time stamp data in relation to files in a file system, the tool must list all date/time data available.

Furthermore, an investigator requires the ability to identify and generate a listing of all deleted files in the file system. Various operating systems handle deleting files in various ways, so the specific capability of a tool will be dependent on the file system the tool is examining, but to some degree, all file systems have a way of at least identifying that a file once existed in a certain space.

Search the Contents of the Regular Files

Searching the contents of the regular files is a particularly important requirement for the search tool. If the search tool opens a regular file to search its contents for a keyword, and that process changes either the file contents or a date/time stamp maintained by the operating system about the file, then the investigator may have to restore an image of the media to get back to the original file contents or date/time stamps. Some search tools that operate at the logical level of the media do not quite meet this requirement, because most operating systems keep a Date/Time Last Accessed time stamp and will attempt to update this stamp when the search tool opens or closes the file.

It is particularly important to test search tools under very controlled conditions to ensure they actually meet this requirement. If a search tool allows the operating system to update Date/Time Last Accessed when the tool runs, then the investigator must take steps to preserve those date/time stamps prior to using the search tool.

An investigator also needs the capability to validate file types where applicable using known header-extension pairs and to hash all the logical files using a recognized and appropriate hashing algorithm. In most cases, the minimum standard at a file level is the CRC algorithm, but for very large files, the MD5 algorithm is preferred.

Ability to Identify and Process Special Files

Special files are in a format in which their contents are either not written to disk or not maintained internally in a readily readable, searchable format. Special files include encrypted, compressed, or password-protected files; steganographic carrier files; graphics, video, and audio files; format files; executable files or binary data files; files housing email archives or active email content; swap files or virtual memory files; and other such file formats that obscure their plain text content. Some password-protected files can be processed in a manner to remove or expose the password. Other types of special files, such as encryption or steganography, may require a more dedicated effort to bypass the security mechanisms.

Recover Pertinent Deleted Files

Recovering pertinent deleted files would logically include a capability to identify and search all file slack. This would also include identifying and searching all free (unallocated) space, identifying relevant file headers in free space, identifying deleted directories in free space, including directory entries for deleted files, and recovering deleted directory entries as well as all pertinent deleted files that are not overwritten.

Make Forensically Sound Images

Once the preview process has identified that certain systems or media contain information relevant to the issues at hand, an investigator must have tools capable of making forensically sound images of those systems or media. The criteria for forensically sound media images is fairly straightforward: the image must include a true, validated copy of every bit of every byte contained on the media, without regard to media contents, from the absolute beginning of the media to the end of the physical device.

The exact mechanism by which that data is retrieved from the evidence media, stored in an image file, and validated will vary, but the image file must contain validated copies of all data from the original media. In today's world of smart cards and "computer memory cards," where cameras can store hundreds of pictures on memory cards (where these cards can supply memory to portable or handheld devices), the variety of media investigators are faced with is ever-widening. Today's media are outdated tomorrow. New imaging and analysis tools must keep apace.

Restore Forensic Images to Suitable Media

Where the functionality of an application is the issue, merely analyzing the files comprising the application at a physical or logical level may not be enough to satisfy the questions. This requirement stems from a need to be able to run applications installed on drives that have been preserved as evidence. For instance, in a fraud investigation, if an investigator needs to print reports from a large financial application installed on a drive that he has imaged, and he no longer has access to the original drives, he may need to restore the image to run the application to print the reports. Today's large applications rely on installation processes that do more than just copy the application files to the media, so running the application in its installed environment may be necessary. This cannot currently be done from within the image files, so the image must be restored.

Perform a Sector-by-Sector Comparison

To verify that one piece of media is an identical copy of another, investigators typically use media hashes of some type. But where two pieces of media are thought to be identical copies of each other, but hash differently, it must be possible to compare sector-by-sector. In most cases, simply knowing that two pieces of media have different hashes will not give you an indication of where on the media the difference occurs. This capability would be especially useful when an investigator must restore an image of a piece of media to a dissimilar piece of media. This tool could verify that any differences between the original and the copy are merely sectors filled with hashes and are accounted for by geometry differences only.

Thoroughly Document Investigative Activities

Thoroughly documenting investigative activities would preferably be an automated part of the forensic analysis software. If the software is self-documenting and certain reports are automatically generated for the user, based on the results of exercising the capabilities of the software, this could help make reporting results much simpler.

Now that we've looked at computer forensics requirements definitions, let's look at digital evidence standards and principles. This next part of the chapter recommends the establishment of computer forensics standards for the exchange of digital evidence between sovereign nations and is intended to elicit constructive discussion regarding digital evidence.

Standards and Principles of Digital Evidence

The latter part of the 20th century was marked by the electronic transistor and the machines and ideas made possible by it. As a result, the world changed from analog to digital. Although the computer reigns supreme in the digital domain, it is not the only digital device. An entire constellation of audio, video, communications, and photographic devices are becoming so closely associated with the computer as to have converged with it.

From a law enforcement perspective, more of the information that serves as currency in the judicial process is being stored, transmitted, or processed in digital form. The connectivity resulting from a single world economy in which the companies providing goods and services are truly international has enabled criminals to act transjurisdictionally with ease. Consequently, a perpetrator may be brought to justice in one jurisdiction while the digital evidence required to successfully prosecute the case may reside only in other jurisdictions.

This situation requires that all nations have the ability to collect and preserve digital evidence for their own needs as well as for the potential needs of other sovereigns. Each jurisdiction has its own system of government and administration of justice, but in order for one country to protect itself and its citizens, it must be able to make use of evidence collected by other nations.

Although it is not reasonable to expect all nations to know about and abide by the precise laws and rules of other countries, a means that will allow the exchange of evidence must be found. This part of the chapter defines the technical aspects of these exchanges.

Standards

To ensure that digital evidence is collected, preserved, examined, and transferred in a manner that safeguards the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system. Standard operating procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and use broadly accepted procedures, equipment, and materials.

Standards and Criteria

All agencies and organizations that seize or examine digital evidence must maintain an appropriate SOP document. All elements of an organization's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.

The use of SOPs is fundamental to both law enforcement and forensic science. Guidelines that are consistent with scientific and legal principles are essential to the acceptance of results and conclusions by courts and other agencies. The development and implementation of these SOPs must be under an organization's management authority.

Management must review the SOPs on an annual basis to ensure their continued suitability and effectiveness. Rapid technological changes are the hallmark of digital evidence, with the types, formats, and methods for seizing and examining digital evidence changing quickly. To ensure that personnel, training, equipment, and procedures continue to be appropriate and effective, management must review and update SOP documents annually.

Procedures used must be generally accepted in the field or supported by data gathered and recorded in a scientific manner. Because a variety of scientific procedures may validly be applied to a given problem, standards and criteria for assessing procedures need to remain flexible. The validity of a procedure may be established by demonstrating the accuracy and reliability of specific techniques. In the digital evidence area, peer review of SOPs by other organizations may be useful.

The organization must maintain written copies of appropriate technical procedures. Procedures should set forth their purpose and appropriate application. Required elements such as hardware and software must be listed, and the proper steps for successful use should be listed or discussed. Any limitations in the use of the procedure or the use or interpretation of the results should be established. Personnel who use these procedures must be familiar with them and have them available for reference.

The organization must use hardware and software that is appropriate and effective for the seizure or examination procedure. Although many acceptable procedures may be used to perform a task, considerable variation among cases requires that personnel have the flexibility to exercise judgment in selecting a method appropriate to the problem.

Hardware used in the seizure or examination of digital evidence should be in good operating condition and be tested to ensure that it operates correctly. Software must be tested to ensure that it produces reliable results for use in seizure and examination.

All activity relating to the seizure, storage, examination, and transfer of digital evidence must be recorded in writing and be available for review and testimony. In general, documentation to support conclusions must be such that, in the absence of the originator, another competent person could evaluate what was done, interpret the data, and arrive at the same conclusions as the originator.

The requirement for evidence reliability necessitates a chain of custody for all items of evidence. Chain-of-custody documentation must be maintained for all digital evidence. Case notes and records of observations must be of a permanent nature. Handwritten notes and observations must be in ink, not pencil, although pencil (including color) may be appropriate for diagrams or making tracings. Any corrections to notes must be made by an initialed, single strikeout; nothing in the handwritten information should be obliterated or erased. Notes and records should be authenticated by handwritten signatures, initials, digital signatures, or other marking systems.

Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner. As discussed in the preceding standards and criteria, evidence has value only if it can be shown to be accurate, reliable, and controlled. A quality forensic program consists of properly trained personnel and appropriate equipment, software, and procedures to collectively ensure these attributes.

Finally, now that the establishment of computer forensics standards has been made, it is time to recommend some auditing techniques. The following auditing techniques are based on how to audit your internal computer forensics and Internet security policies.

Computer Forensics Auditing Techniques

Companies that believe their networks and the Internet can be completely protected by a phalanx of add-on computer forensics and security products may be in for a rude awakening. Underlying vulnerabilities, embedded and unseen many layers down in network infrastructures and the Internet, may be unwitting invitations to even moderately skilled attackers.

Computer forensics and security-auditing companies can give a company expert analysis of obscure but potentially devastating loopholes, along with estimates of cost versus risk for each of many possible approaches to address them—and a basis for deciding whether spending a little more money up front will save much more in the long run. This last part of the chapter makes some recommendations into how computer forensic and security auditors go through a network and what steps are necessary for companies to lock down their networks—especially the ones that are connected to the Internet.

How to Audit Your Network and Internet Security Policies with Computer Forensics Techniques

The Internet has allowed businesses to communicate in new and strategic ways with various types of people and organizations. System administrators do not have to argue for an Internet connection anymore. Instead, they have to fight for the resources to secure it. Auditing your Internet and network security with computer-forensics techniques is a responsibility that should be frequently revisited and improved, and you should not hesitate in dedicating resources to security when you find shortcomings.

The Internet Octopus

Over the years, you have added feature upon feature to your Internet and network connections. As needs have changed, you have found yourself needing more robust services, faster connections, and more flexibility in what can be done. In the beginning, services such as simple POP3-style email and Web access were the extent of an Internet connection. Today, you have site-to-site Virtual Private Networks (VPNs); client-side and home-user VPNs; streaming media; Web-based training; company Web sites; Internet applications; e-commerce [4]; and business-to-business extranets. During all these changes in the past few years, you have probably changed IT personnel, Internet platforms, and network connections at least once. This scenario makes it easy to have some unforeseen, yet preventable, exposures.

Any network connection to the Internet is vulnerable to exploitation. The most basic vulnerability that all network connections face is that they could be made unavailable and bring down mission-critical services with them. Today, you are finding more intelligent defenses against attacks, such as denial-of-service attacks, as routers and other devices can be set to verify source addresses and ignore packets if they are bogus or carry a suspicious pattern. However, beyond the denial-of-service category of vulnerabilities, there are always the standard concerns of open ports, easy passwords, unsecured routers, and unknown “features” that any Internet device may have.

Many organizations have grown their Internet set of features across multiple devices or possibly multiple network connections—a firewall for Web and email traffic, a VPN appliance for remote connections, a different firewall for a business-to-business relationship, or other possible combinations of lines and devices that can push Internet vulnerabilities beyond control. These services can even be distributed across multiple Internet connections or across multiple Internet service providers. Regardless of the number of devices that are on the Internet, each has different services that can be potentially exploited. You can see how an enterprise environment such as this could quickly become difficult to manage from a security standpoint.

What You Can Do

There are a number of things you can do to keep your network connections secure and to keep business running as usual. One of the easiest measures you can take is to clean things up:

- Verify that there are no accounts for terminated employees.
- Check for any manufacturer or service provider default passwords that may be easily known or guessed.
- Verify that any temporary services or open ports are disabled.
- Beware of potential internal threats.
- Have the mindset of "deny all except that which is explicitly stated in the rule set."

After this basic housekeeping is completed, it's important to perform a "vulnerability chain assessment" with your computer forensics tools on your own. This will allow you to gauge the entire scope of an Internet and network security policy. A vulnerability chain assessment tells administrators what is affected by what and who potential perpetrators could be.

All the items listed below have vulnerabilities—some of which are beyond your control. For each item, consider the potential vulnerabilities that could cause an interruption of service:

Internet (outside of your router): Internet being unavailable from your carrier or region, phone line cut, denial of service, and so on.

Internet line: Physical disconnection—via a perpetrator or the carrier.

Internet router: ISP configuration may have well-known default passwords; this could reroute all incoming mail, shut down an interface, or adversely affect performance by some other means.

Internet/external network: If this segment is a managed device (hub, switch, or other), it could be falsely managed to disable ports or could be affected by the failure of the device.

VPN appliance and firewall: Security compromise, stale VPN accounts or vendor default account, unwanted services, failure of device, and so on.

Internal network: Failure of any internal device, internal security threats on interior devices to the Internet, and the like.

Obtain Peace of Mind

One thing you can do to bring some validity to your efforts is to get an external opinion of your Internet and network security. You can obtain this opinion via:

- A formal Internet and network security audit from a person or organization with certified information system auditor (CISA) and computer forensics certification.
- A third-party piece of computer forensic auditing software or original equipment manufacturer (OEM-provided) tool to examine security issues.
- A professional hacker trying to compromise an Internet presence.

The professional hacker approach is recommended, but you have to be careful. These types of companies need to be true DEF CON followers and really know their stuff. You want a professional hacker to do more than call vendors asking for passwords and back-door methods.

Many general IT vendors offer intrusion detection or an Internet exposure analysis. These third-party computer forensic examinations can yield beneficial information to solidify a security strategy. One of the benefits provided is when they attempt to exploit vulnerabilities (although they will not actually destroy data or compromise systems) and demonstrate how much damage they could do by how far they're able to get in. It's a wonderful feeling to present management with a report saying that this external group is impressed with the security of your Internet presence.

Continued Monitoring and Risk Distribution

You can solidify your security strategy by constantly monitoring it and by keeping up with the latest computer-forensic and hacking tools and methodologies. You can also find Web sites that host information on how to exploit specific products. These are usually based on out-of-the-box configurations, so keep current with vendors on new features, versions, or newly exposed risks.

There are countless free or time-trial pieces of computer forensics auditing software you can use to peek at your connection, but be careful. These tools may be dangerous to your operating environment, so a test computer is ideal for such computer forensic investigations.

One of the things that is also very important is your ability to distribute risk. That's rather easy, actually. However, the better you distribute risk, the more expensive things become. Here are some recommended risk distribution tips:

- If you need firewall and VPN services, consider having those on two different devices—from different vendors.
- Have an alternate Internet connection. If another ISDN or T1 line is not possible, consider testing the alternate serial interface of a router that may be configurable to dial a modem.
- Put up a honeypot to attract or distract would-be hackers. Give it a registered DNS name such as lotusnotes.company.com but don't host anything on it.

- Proactively renew or cancel your Internet service provider agreement before it expires or before the carrier contacts you. Do not assume that they will continue to bill you at the current rate or that someone will call you to discuss options.

With a bit of diligence, you can keep your Internet and network security at peak, which will protect the business goals of the organization. Hopefully, this final chapter has provided some fresh ideas on keeping security first.

FINAL WORD: COMPUTER FORENSIC NEEDS AND CHALLENGES

Reporting of economic and cyber crime is problematic and grossly underestimated, as is apparent from the many risks associated with corporations' reporting or sharing fraud losses and activity. A uniform computer forensics crime reporting system should be developed that includes specific economic crimes.

The Fraud Identification Codes established by the National Fraud Center are a start. Until such a means of a computer forensics crime-reporting system is implemented and the stigma of fraud victimization is removed, this problem will not be solved. Uniform and thorough reporting is necessary in the war on economic and cyber crime; resources for computer forensics investigation and prosecution will naturally follow as the enormity of the problem unfolds.

The lack of agreed-on definitions regarding economic crime and computer crime has resulted in a paucity of data and information on the size and scope of the problem. Academics have not been able to agree on definitions and have, for the most part, continued to focus on white-collar crime.

Economic crime is defined as an illegal act (or a constantly evolving set of acts) generally committed by deception or misrepresentation (fraud) by someone (or a group) who has special professional or technical skills for the purposes of personal or organizational financial gain or to gain (or attempt to gain) an unfair advantage over another individual or entity. To this day, the true nature of the amount of economic crime is buried in the statistics of more conventional crimes. For example, credit-card fraud is typically classified as larceny instead of access-device fraud.

Preventing, detecting, investigating, and prosecuting economic crimes must become a priority in order to lessen their impact on the economy and the public's confidence. Law enforcement, as it stands now, is in danger of slipping further behind the highly sophisticated criminals. New resources, support for existing organizations (the National Fraud Center, the National White Collar Crime Center, the IFC, and the Economic Crime Investigation Institute), and innovative computer forensics solutions are needed to control this growing problem in the United States and the world.

These computer forensics needs and challenges can be accomplished only with the cooperation of the private, public, and international sectors. All stakeholders must be more willing to exchange information on the effect economic and cyber crime has on them and the methods they are using to detect and prevent it.

No single sector holds all the computer forensics resources, tools, or solutions. In fact, industry has more resources than government, but it must be motivated and authorized to partner and communicate. All parties must be willing to work together to effect change in existing laws and regulations and to promulgate new initiatives. The victims need to follow the lead of the criminals and organize themselves, so that the organized bad guys are not operating in a lawless environment, where culpability is at a minimum.

The United States must take the lead. Current and future administrations must recognize the full impact of economic and cyber crime, both domestically and globally, and make a concerted, strategic effort to combat it, for the benefit of all society.

Finally, let's move on to the real interactive part of this chapter: review questions and exercises. The answers and solutions by chapter can be found in Appendix E.

CHAPTER REVIEW QUESTIONS AND EXERCISES

True/False

1. True or False? When dealing with digital evidence, all the standard forensic and procedural principles must not be applied.
2. True or False? Upon seizing digital evidence, actions taken should not change that evidence.
3. True or False? People who access original digital evidence should not be trained for the purpose.
4. True or False? All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
5. True or False? Individuals are responsible for all actions taken with respect to digital evidence while such evidence is in their possession.

Multiple Choice

1. To help create cooperation between the United States and other nations, the G8 group of major industrialized nations has proposed six principles for procedures relating to digital evidence, which it defines as *information stored or transmitted in binary form that may be relied on in court*:

A. When dealing with digital evidence, all the standard forensic and procedural principles must be applied.
B. Upon seizing digital evidence, actions taken should not change that evidence.
C. People who access original digital evidence should be trained for the purpose.
D. All activity relating to the seizure, access, storage [1], or transfer of digital evidence must be fully documented, preserved, and available for review.
E. Individuals are not responsible for all actions taken with respect to digital evidence while such evidence is in their possession.

2. It is recommended that the following capabilities are useful as a starting point to develop a set of minimum requirements:

A. An investigator requires a capability to simultaneously preview a large number of systems on site to determine which ones contain relevant evidence.
B. An investigator requires the capability to conduct a search at the physical level of the target media, ignoring operating system and file system logical structures, and searching from sector 0 to the end of the media regardless of the logical content.
C. The search tool must be able to unreliably report the physical location on the media where responsive data were found.
D. An investigator requires the capability to conduct a thorough, read-only search at the logical level of the target media.
E. An investigator requires an ability to generate a listing of all logical files in a file system.

3. There are a number of things you can do to keep your network connections secure and to keep business running as usual. One of the easiest measures you can take is to clean things up, except:

A. Verify that there are no accounts for terminated employees.
B. Check for any manufacturer or service provider default passwords that may be easily known or guessed.
C. Verify that any temporary services or open ports are disabled.
D. Beware of potential external threats.
E. Have the mindset of "deny all except that which is explicitly stated in the rule set."

4. All the items listed below have vulnerabilities—some of which are beyond your control. For each item, consider the potential vulnerabilities that could cause an interruption of service, except which one:

A. Internet (outside of your router)
B. Internet line

C. Internet router
D. Internet/external network
E. VPN appliance and IDS

5. One thing you can do to bring some validity to your efforts is to get an external opinion of your Internet and network security. You can obtain this opinion via the following, except:
   A. A professional hacker trying to compromise an extranet presence.
   B. A formal Internet and network security audit from a person or organization with CISA and computer forensics certification.
   C. A third-party piece of computer forensic auditing software or OEM-provided tool to examine security issues.
   D. A professional hacker trying to compromise an Internet presence.

Exercise

When a leading United States–based drug manufacturer's financial audit team received a tip that certain employees were suspected of performing fraudulent actions, they responded immediately by launching a full-scale investigation. This investigation presented significant but common challenges faced by global enterprises committed to addressing internal fraud. First, the fraudulent activity was occurring on the other side of globe at the company's Middle East office. Secondly, as is typically the case, almost all of the critical evidence was in digital format, stored on the hard drives of the workstations and servers at the site. Traditionally, an effective investigation would require the investigation staff to travel to the remote location. Such costly travel and disruptive activity would likely compromise the integrity of the investigation and could even lead to destruction of evidence by the suspects. In addition to fraud having a potentially serious impact on a company's bottom line, Sarbanes-Oxley mandates that public companies have a diligent, internal fraud investigation capability. It was imperative that this investigation be handled in a professional and effective manner. This required the diligent and thorough investigation of all relevant Middle East–based computer activity, which could not be performed by local IT staff, as they were potential suspects. Because this case called for specific and extensive IT expertise, company auditors began their investigative process through the company's United States–based corporate computer forensics specialist team (CFST). How was the CFST able to go about conducting their investigations?

REFERENCES

[1] Vacca, John R., *The Essential Guide to Storage Area Networks*, Prentice Hall, New York, 2002.

[2] Gottfried, Grant, "Emerging Technology: Taking a Byte Out of Crime," National Center for Forensic Science (NCFS), Orlando, FL, 2002.

[3] Vacca, John R., *Net Privacy: A Guide to Developing & Implementing an Ironclad ebusiness Privacy Plan*, McGraw-Hill, New York, 2001.

[3a] "2004 Computer Crime and Security Survey," Computer Security Institute of San Francisco and the FBI, 2004.

[4] Vacca, John R., *Electronic Commerce,* 3rd ed., Charles River Media, Hingham, MA, 2001.

This page intentionally left blank

A Frequently Asked Questions

WHAT IS COMPUTER FORENSICS?

Computer forensics is the collection, preservation, analysis, and court presentation of computer-related evidence.

WHY COMPUTER FORENSICS?

The vast majority of documents now exist in electronic form. No investigation involving the review of documents, either in a criminal or corporate setting, is complete without including properly handled computer evidence. Computer forensics ensures the preservation and authentication of computer data, which is fragile by its nature and can be easily altered, erased, or subject to claims of tampering without proper handling. Additionally, computer forensics greatly facilitates the recovery and analysis of deleted files and many other forms of compelling information normally invisible to the user.

WHAT IS DATA RECOVERY?

Data recovery is the process of retrieving deleted or inaccessible data from failed electronic storage media such as computer hard disk drives, removable media, optical devices, and tape cartridges. Your data can become inaccessible because of a software problem, computer virus, mechanical or electrical malfunction, or a deliberate human act. Regardless of the cause of your data loss, your experienced technicians should be able to successfully recover lost data 80 to 85% of the time.

How Long Does Data Recovery Take?

Standard Data Recovery

Most recoveries will be completed in 2 to 5 days.

Expedited Data Recovery

If you should need this service, you need a dedicated technician assigned to your drive within 4 hours of the time that you send in your hard disk. This process will normally cut your turnaround time in half.

Emergency Data Recovery

If your situation is critical, you will need to make arrangements for a technician to be available who will be assigned to work on your recovery until it is completed. The goal here is to return your data to you within three to five working days. However, because of the complexity of data recovery, there will be times when it will take longer.

ARE THERE INSTANCES WHEN DATA CANNOT BE RECOVERED?

Yes. There are instances when the damage to the hard drive is so severe that data recovery is not possible. This usually occurs when the read/write heads actually "crash" and gouge the magnetic storage media to the point where the data is destroyed.

However, in a number of cases, data recovery was possible at the time the damage first occurred, but the data became nonrecoverable through the use of commercial recovery software. This software is designed to recover data from working drives. If your drive has experienced a mechanical or electrical failure, the use of recovery software can cause permanent loss of your data.

What Can I Do to Protect My Data and Minimize My Chances of Losing Data?

The adage in the industry is not "if my drive fails," but, rather, "when my drive fails." Although your hard drive has many electronic components, it also has moving parts. Over time, these mechanical components can fail as the result of use.

Avoid Heat and Vibration

All drive components, both electronic and mechanical, are sensitive to heat and vibration. Keep your computer in a dry, controlled environment that is clean and dust-free. Set up your computer in an area with little traffic to ensure that it does not get bumped. Heat and vibration are two of the leading causes of hard drive failure. Also, beware of static.

Back Up Your Data

The surest way to avoid data loss, even if your hard drive fails, is to back up your data. If you don't have a tape backup device or network drive at your fingertips, back up your most important files to a floppy disk at least once a week.

To Avoid Premature Drive Failure, Run Scandisk

Scandisk examines your hard disk for logical inconsistencies and damaged surfaces. Run it every two or three weeks just to be safe. It is important to save any changes to a floppy until you are sure that the changes you are about to make will not adversely affect your hard drive.

Run Defrag Frequently

Files will most likely not be stored in adjacent clusters. Defrag rearranges the data on your hard disk so that each file is stored in a set of contiguous clusters. This is essential for data recovery because success is more likely when the damaged file's clusters are adjacent to each other.

Antivirus Software

Use antivirus software and update it at least four times a year. Also, use an uninterrupted power supply (UPS). In the event of a surge of electricity, black out, brown out, or lightning strike, a UPS can protect your system from electrical damage. A UPS is also a backup power source that keeps your computer running for a short period of time, giving you the opportunity to properly save your work and shut down, avoiding a potential data loss.

Be Cautious When Using Recovery Utilities

Use diagnostic and repair utilities with caution. Verify that your utility software is compatible with your operating software. Never use file-recovery software if you suspect an electrical or mechanical drive failure. Always make an undo disk when you allow a utility to make changes to your hard drive.

How Do I Ship My Hard Drive?

It is extremely important that your hard drive is packaged carefully to avoid any additional damage during shipment. Only your drive is required for data recovery.

Packaging the Hard Drive

Wrap the hard drive in an antistatic material. If an antistatic bag is not available, a freezer bag will suffice. It is recommended that you ship the drive in its original manufacturer's packaging. If this is not possible, pack the hard drive in a sturdy corrugated cardboard box twice the size of the drive, with heavy foam padding, bubble wrap, or other antivibration materials. Do not use styrofoam peanuts, as they attract static electricity. Be sure the padding material is at least two inches thick around the drive.

Water-Damaged Hard Drives

If your drive has suffered water damage, please do not dry it. Enclose the drive along with a damp sponge in a sealed plastic bag to prevent it from drying out.

Controller Boards

When recovering data from older models, you may need to send the controller along with the drive. Remove the controller carefully, enclose in it antistatic material, and ship it along with the drive.

Other

Package all other types of media following the guidelines in the preceding for a typical hard drive.

Locations

Ship the drive directly to the recovery facility nearest you: It is recommended that you ship via UPS or Federal Express domestically and DHL internationally, using next-day service. If you elect to use another carrier, it is suggested that you use an overnight service. Also, if you have any special shipping considerations, questions, or concerns, please contact your overnight carrier.

How Do I Get My Data Back?

If your drive is repairable, the repair will be completed and your data returned to you on your original drive. When your data is recovered and your drive is not repairable, there are many different ways to return your data, including a new drive, magnetic tapes, Zip cartridges, or CD-ROM.

B Computer Forensics Resources

Disclaimer: *This author and publisher do not endorse the contents of the links in this Appendix. They are offered as resources that other systems security and forensics professionals have found helpful.*

GENERAL FORENSICS RESOURCES

AccessData (http://www.accessdata.com/)

Known best for their Password Recovery Toolkit. AccessData's site offers information about this and other security-related tools, and you will find several free tools here. Also, you will find several articles and links regarding cryptography and related subjects.

Digital Intelligence, Inc. (http://www.digitalintelligence.com/)

Digital Intelligence designs and builds computer forensic software and hardware. They also offer free forensic utility software for law enforcement.

Fred Cohen & Associates (http://all.net/)

This site is full of network security and information warfare articles and white papers. Fred Cohen is one of the most recognized, respected, and requested names in information protection today.

Guidance Software (http://www.guidancesoftware.com/)

Guidance is the creator of the popular GUI-based forensic tool EnCase. Besides information regarding their EnCase forensic tool, there is a bulletin board with a number of forums relating to their products and computer forensics.

High Tech Crime Investigation Association (http://htcia.org/)

This is an association that promotes the exchange of data and ideas about methods relating to investigations and security among its membership.

International Association of Computer Investigative Specialists (http://cops.org/)

IACIS is an international, volunteer nonprofit corporation composed of law enforcement professionals dedicated to education in the field of forensic computer science.

Mares and Company, LLC (http://www.dmares.com/)

Mares has been authoring computer forensic tools for law enforcement for many years. This site provides access to all his tools as well as a number of articles and papers relating to computer forensics. Information regarding Mares' computer forensic training can also be found on this site.

NTI—Computer Evidence Leaders (http://www.forensics-intl.com/)

NTI has a comprehensive suite of computer forensic tools that have been used by law enforcement for many years. There are also many good articles concerning technical and legal issues surrounding computer forensics.

Porcupine.org (http://www.porcupine.org/wietse/)

This site is provided by Wietse Zweitze Venema, which provides tools and white papers focused primarily on postmortem analysis of computer break-ins.

Sydex Inc. (http://www.sydex.com/)

Sydex can take hundreds of different floppy and tape types and convert them to Windows-readable files. They use their own specially designed equipment to process just about any format. They can also repair diskette data errors and perform forensic analysis. They've written forensic software that's been in use for years by many government and private organizations.

The Coroner's Toolkit (http://www.fish.com/tct/)

The Coroner's Toolkit is a collection of tools that are oriented toward either gathering or analyzing forensic data on a Unix system.

TUCOFS (http://www.tucofs.com/tucofs.htm)

The TUCOFS Web site is a great collection of computer forensics resources and tools.

Interpact, Inc. (http://www.infowar.com/)

The sole purpose of this site is for information warfare and computer security.

WetStone Technologies, Inc. (http://www.wetstonetech.com/page/page/1097778.htm)

WetStone Technologies is a developer of information security technologies. This site includes some excellent technical papers concerning advancing crime scene computer forensics, timelining computer evidence, and using smart cards and digital signatures to preserve electronic evidence.

COMPUTER CRIME

Center for Democracy and Technology (http://www.cdt.org/policy/terrorism/)

The Center for Democracy and Technology works to promote democratic values and constitutional liberties in the digital age. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

FILE FORMATS AND EXTENSIONS

Computer Knowledge (http://filext.com/)

File extensions are often used to determine the program that created the file. Although there is no guarantee that users will not rename files or associate odd extensions with particular programs, this site lists some fairly standard associations.

Wotsit's Format (http://www.wotsit.org/)

This site contains file format information, including header/foot signatures, on hundreds of different file types and all sorts of other useful programming information: algorithms, source code, specifications, and so on.

CRYPTOGRAPHY AND STEGANOGRAPHY

Counterpane Internet Security, Inc. (http://www.counterpane.com/)

An outstanding site about cryptography containing numerous technical papers about the subject. Free tools can also be found here. Counterpane Internet Security, Inc. offers leading-edge expertise in the fields of 24/7 intrusion detection and prevention, preemptive threat discovery, forensic research, and organizational IT systems analysis.

Steganalysis–Attacks Against Steganography and Watermarking–Countermeasures (http://www.jjtc.com/Steganalysis/)

An excellent site about steganography and steganalysis. Includes white papers on steganalysis and countermeasures among other things.

CAUTION

URLs are subject to change without notice.

C Links to Computer Forensics and Related Law Enforcement Web Pages

Disclaimer: *This author and publisher do not endorse the contents of the links in this Appendix. They are offered as resources that other systems security and forensics professionals have found helpful.*

LAW ENFORCEMENT LINKS

Computer Crimes and Technology Links

http://www.co.pinellas.fl.us/bcc/juscoord/ecomputer.htm

Computer and Internet Security Resources

http://www.virtuallibrarian.com/legal/

Mitretek Systems

http://www.mitretek.org/Home.nsf/Main/BusinessAreas

Internet Resources on Technology Law

http://www.bitlaw.com/

Ira Wilsker's Law Enforcement Sites on the Web

http://www.ih2000.net/ira/ira.htm

Law Enforcment Guide to the World Wide Web

http://www.leolinks.com/

Legal and Court-Related Sites

http://www.ih2000.net/ira/legal.htm

Mega Links in Criminal Justice

http://faculty.ncwc.edu/toconnor/

The Police Officer's Internet Directory

http://www.officer.com/

Web of Justice Links

http://www.co.pinellas.fl.us/bcc/juscoord/explore.htm

What's on the Internet for Legal and Law Enforcement Personnel

http://www.knock-knock.com/forensic.htm

ORGANIZATIONS

High Tech Crime Cops

http://www.hightechcrimecops.org/

International Association of Computer Investigative Specialists

http://www.cops.org/

MAILING LISTS

High Tech Crime Cops List

http://groups.yahoo.com/subscribe.cgi/htcc

USDOJ GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS

Main Table of Contents

http://www.usdoj.gov/criminal/cybercrime/search_docs/toc.htm

Update to USDOJ Guidelines

http://www.usdoj.gov/criminal/cybercrime/supplement/ssgsup.htm

COMPUTER FORENSIC AND SECURITY SOFTWARE AVAILABLE FREE OF CHARGE TO LAW ENFORCEMENT AGENCIES

New Technologies, Inc.

http://www.forensics-intl.com/download.html

MISCELLANEOUS

Berryhill Computer Forensics

http://www.computerforensics.com/index.htm

Computer Expert and Computer Forensics Consultant–Judd Robbins

http://www.computerforensics.net/

Computer Forensics Expert Witness Network

http://computerforensics.net/

Computer Forensics FAQ

http://www.surveil.com/frequent.htm

Computer Forensics Online

http://www.shk-dplc.com/cfo/

Florida Association of Computer Crime Investigators

http://facci.org/

The Risk Advisory Group Limited–Investigations

http://www.riskadvisory.net/index.html

CCIPS Searching and Seizing Computers

http://www.usdoj.gov/criminal/cybercrime/searching.html

FDIC: Law, Regulations, Regulated Acts–Miscellaneous Statutes and Regulations netForensics Home Page

http://www.fdic.gov/regulations/laws/rules/8000-900.html

Infowar, Info-Sec Portal, Information Warfare and Security Global Clearinghouse, Cyber Crime Reporting

http://www.infowar.com/

FOCUS on Incident Handling: An Introduction to the Field Guide for Investigating Computer Crime

http://www.securityfocus.com/focus/ih/articles/crimeguide1.html

FOCUS on Incident Handling: Overview of a Methodology for the Application of Computer Forensics

http://www.securityfocus.com/focus/ih/articles/crimeguide2.html

FOCUS on Incident Handling: Digital Media Forensics

http://www.securityfocus.com/focus/ih/articles/dforensics.html

FOCUS on Intrusion Detection: Know Your Enemy: A Forensic Analysis

http://www.securityfocus.com/focus/ih/articles/foranalysis.html

SMO: Legal Reporter 06/00

http://www.securitymanagement.com/library/000873.html

CAUTION

URLs are subject to change without notice.

D More Computer Forensics Cases

Claims of six-figure salaries earned without ever leaving the bedroom. A hearty supply of free computer hardware and a never-ending mail inbox full of victims. Credit-card accounts fished from fake porn sites or clever emails promising "You've Got Pictures" that ask for AOL user names and passwords. What do computer criminals do all day? Work the system—and reap the rewards.

So, what's been the result? Fraud and credit-card theft have run rampant on the Internet, and in-house corporate thieves abound. The following are some additional computer forensics case studies for your reading enjoyment and horror.

CASE STUDY 1: LOST FILES

A set of Word, Excel, and Project files that was created over 18 months relating to a project currently under construction has been maliciously deleted by a departing employee. The PC was not backed up. The action was discovered 3 days later and the IT group endeavored to locate and restore the files. They were unsuccessful. Management is assessing the options available. They are time consuming and expensive. Some data cannot be rekeyed in because the source data is missing. The IT manager contacts a computer forensics firm. The firm finally restores the entire project directory within 4 days from first contact.

CASE STUDY 2: CORRUPTED FILES

Files relating to a multimillion tender on a sales and marketing PC have been found to be corrupted. The PC was not on the network and not backed up. The IT group advises that the data is gone forever. The tender closes at the end of the month, which is only 12 days away. Management is assessing the options available. The only option appears to be to withdraw from the tender process. Their hardware supplier recommends an inquiry to a computer forensics data-recovery firm. The firm receives the hard disk at 4:00 P.M. on Friday and has a CD-ROM containing the draft tender response, worksheets, subcontractor quotations, graphics files, and peripheral material on the client's premises by 11:00 A.M. on the following Monday.

CASE STUDY 3: DISAPPEARING FILES

The debtors module of an accounting package has somehow disappeared from the accounting PC. The software-support company is unable to locate the files, and the backup tapes do not restore correctly. The software-support company suggests that the data be rekeyed in—a massive task. Management is assessing their options. They are time-consuming and expensive. The distributor of the software recommends contact be made with a computer forensics firm. The firm finally restores the faulty data in time for the complete end-of-month statement run.

CASE STUDY 4: COMPUTER FORENSICS

The founder and majority shareholder of a consultancy business sold his interest to a multinational communications corporation. The contract of sale contained restraint clauses, prohibitions on the removal of confidential information, and nonsolicitation of staff and client clauses. After about a year, the client—the multinational—became suspicious that he was acting in breach of contract. A computer forensics firm was asked to investigate. At the outset, the firm suggested that the individual's desktop and laptop computers be recovered to copy the hard disks and analyze their contents. Within an encrypted file on his desktop, the firm found a draft business plan for a new enterprise that would compete with his former business. On his laptop, in a deleted file that was restored, the firm recovered details of key clients and revenue streams. It was possible to demonstrate that information had been updated within these files after he had left the company, but before he had returned the computer. Taken together, the evidence was sufficient to initiate criminal proceedings.

CASE STUDY 5: FORENSIC ACCOUNTING

A multinational manufacturer reported significant losses in the company's distribution division. It was not clear whether this was simply a result of an inequitable transfer pricing policy within the group or whether the company had been defrauded. Accountants from a computer forensics firm set out to investigate how the losses had been incurred, reconstructing incomplete records and unraveling a confusing series of transactions. They discovered that other companies within the group had transferred products to the division at over market value to maintain their own profitability. More disturbingly, the division had sold much of its product at inexplicably low prices to a number of key customers. The business manager was dismissed after the computer forensics firm discovered that he had concealed ownership interests in some of these customers and evidence came to light indicating that he had accepted kickback payments. Poor and missing records prevented legal action from being commenced. In the following period, the division was on track to report profits following tighter controls over transfer pricing and sales invoicing.

CASE STUDY 6: CORPORATE INVESTIGATION INTO PC PORNOGRAPHY

A computer forensics team was contracted to assist in an investigation for an organization that suspected an employee of downloading and storing inappropriate material on a company PC. The team visited the site and, using correct forensic procedures, created an image of the hard drive of the suspect PC. The team was then able to recover a large amount of inappropriate material from the PC in a forensically sound manner, including files that had been deleted, renamed, and hidden in an attempt to disguise their true nature. Using this evidence and the report the team produced, the client was able to take the appropriate action against the employee.

CASE STUDY 7: DATA RECOVERY

A computer forensics team was asked to assist an organization that had lost data as a result of a computer virus. The affected laptops were with field personnel and away from the central office when the virus was introduced. Consequently, the data collected over this period had not been backed up. The affected machines were brought to the team's secure laboratory, and, using forensic recovery techniques, they were able to image data from the affected machines, recover all of the data that had been stored since the machines had last been backed up, and eliminate the virus.

CASE STUDY 8: INDUSTRIAL ESPIONAGE

A computer forensics team was asked to assist in a case where it was suspected that industrial espionage had taken place through the computer system. It was suspected that a number of techniques had been used to plant spyware (remote control and covert information-gathering programs) on a network. After carrying out a preliminary on-site analysis, the team removed a number of suspect machines to their secure laboratory for further analysis. A number of machines had been compromised after employees had opened email attachments that contained trojan horse programs (programs that are disguised as common files but actually contain malicious code). Unfortunately, these had been missed by the organization's antivirus measures. As an added service, the team's security engineers were able to offer advice and assistance in reconfiguring antivirus and firewall products to minimize the chance of a repeat occurrence.

CASE STUDY 9: FAMILY MEMBERS BOLT

Family members bolt, take the IT department and the product design, sabotage the originals, and go into competition. A family-owned product manufacturer and designer on the verge of being bought for many millions of dollars found most of its designs missing after the departure of key managers and designers. A program used for deep file destruction had been implemented to destroy both product designs and evidence of the procedure itself. An outside computer forensics consultant is brought in to recover designs and overwrites evidence instead. A computer forensics team is then brought in and discovers remnants of file destruction utility and data patterns consistent with sabotage by the same utility. The suspects finally admitted to the use of the utility.

CASE STUDY 10: FORMER EMPLOYER

A former employer claims a competitor's new hire has stolen designs for manufacture. An individual working for a biomaterials firm gained employment with a competing firm. The individual had used several dozen diskettes for storage at the old firm and then used the same diskettes for new storage at the new firm. The previous employer claimed that the individual took designs to the new employer on diskettes. A computer forensics team was engaged to demonstrate the employee's innocence. The original firm finally settled out of court.

CASE STUDY 11: GOODS LEFT TO ROT

Goods were left to rot while documents were allegedly backdated. A computer forensics team was hired to check the results of a police report that suggested the client's guilt. The client's attorney was advised as to the potential veracity of the claim. Inconsistencies in the police report were discovered, and the sentence was mitigated.

CASE STUDY 12: MANAGERS START NEW COMPANY

Managers start a new company in the very offices of their employers; computers and backups disappear. A foreign branch of the entertainment arm of a multinational conglomerate suspects that key managers had been attempting to incorporate company intellectual assets into a competing product line. Once the suspects believed they were under suspicion, the relevant office computers were reported as stolen. Data backups were reported as missing. Under pressure, the original computers were found and produced by a computer expert among the suspect group, but with large amounts of data missing. A computer forensics team was hired to investigate. Unequivocal evidence of illegal activities was produced from the remains of files on the computers in question.

CASE STUDY 13: FAMILY MEMBER STEALS CLIENTS

A member of a family-run communications business left the company. While denying it, the individual started a business in direct competition with the family business. The individual's computer was identified as an asset of the original company. The individual claimed that no company information was on the computer. A computer forensics team was hired to test the claim. Although the computer had been completely deleted, reformatted, and had entirely new operating systems and applications installed on it, the original database entries were, nonetheless, uncovered. The individual also claimed innocence up until the moment that the team experts were seen awaiting a call into the courtroom. The individual then admitted the wrongdoing and settled.

CASE STUDY 14: ERASED EMAIL

A private investigation firm was purchased, with a covenant by the previous owners not to compete. Within weeks, suspicion arose that the covenant was not being respected and that files and media that had been turned over had data removed. A computer forensics team was hired to look into the matter. Thousands of files were turned up by the investigation, showing a violation of the covenant.

CASE STUDY 15: BANK SUSPECTS

An employee of an FDIC-insured bank turned over a computer upon exiting from his employer. The managers suspected that this individual had revealed confidential information regarding loan clients and credit information A computer forensics team was hired to inspect the email server records for deleted email files that might cast light on the individual's actions. In short order, the text of the suspect emails, which showed the former employee's culpability was revealed.

CASE STUDY 16: FORMER MANAGERS

Several managers left a software-design firm. Within a few weeks, they started up a new firm, producing similar products, in direct competition with the original firm. A computer forensics team was hired to inspect former managers' computers, which had been erased. Evidence that the business plan and designs for a new firm were taken directly from the original firm was uncovered. The new firm was enjoined by the court from offering their product until sufficient time had passed for them to have produced their own designs. The former managers were given a 9-month injunction.

CASE STUDY 17: FORMER CATALOG DESIGNERS

A company that had spent years producing a catalog and selling thousands of industry-specific parts found that a competing catalog with identical drawings and designs had been produced in a scant few weeks by a new competitor. A computer forensics team was hired to show that the designs of the new company were stolen from the original company. After the findings were presented to a court showing the original company's artwork and text being used in new catalogue, the new company was enjoined from using designs for several months.

CASE STUDY 18: MODEL PURSUED

A wealthy suitor financed a young model. Once the model soured on the suitor, evidence was presented to show that the model had committed libel. Inspection of the model's office computer was ordered. A computer forensics team was hired to attend the inspection only to find that the aforementioned suitor's computer forensic consultants did not understand how to access the data on the computer in question. With advice from the computer forensics team, an inspection was effected. With further advice from the team, it was shown that any suspect email was liable to have been forged by employees of the suitor. The suitor finally settled out of court.

CASE STUDY 19: ENCRYPTED MAIL

A former employee encrypted an email record, address book, and calendar to hide information from an employer. A computer forensics team was hired. The team then successfully cracked the file's encryption and revealed its contents.

CASE STUDY 20: TWO ATTORNEYS CAN'T SPEAK CIVILLY

Two attorneys couldn't speak civilly to each other. A computer forensics team was hired to act as a neutral expert when opposing attorneys did not trust results of each other's experts. The team brought the voice of reason to an acrimonious meeting between attorneys, and calm prevailed while the truth of the matter was revealed in the computer inspection.

CASE STUDY 21: BIG REAL ESTATE DEAL

The manager of a real estate fund was accused of increasing the value of shares in the fund by providing false information to potential investors when the value of the fund plunged. The manager was further accused of faking and falsely dating computer documents to support the claim of innocence. A computer forensics team was hired. Information that was recovered by the team mitigated and diminished claims against the client.

CASE STUDY 22: DOCTOR ACCUSED

A doctor was accused of withholding treatment based on the ethnicity of the accuser. A computer forensics team was hired to inspect hospital records of treatment and meetings to support the medical provider's innocence. Deep inspection of all relevant computers and servers showed no evidence of wrongdoing.

CASE STUDY 23: FORMER EMPLOYEE CLAIMS

A former employee claims he never took any information with him when he left. The firm suspected the former employee of absconding with proprietary information. Under court order, the individual turned over a laptop computer, with no obvious data related to the case. A forensic inspection by a computer forensics team revealed enough relevant data to print two entire reams of documents. The suspect finally settled.

CASE STUDY 24: EX-PARTNER CLAIMS

A partner in an information technology firm left and went into his own business. The individual was accused of taking proprietary documents on his laptop. The individual produced the laptop, along with the claim that, although there were missing documents, none were relevant to the claims. Additionally, the individual claimed that a prolific virus had destroyed the documents. A computer forensics team was hired and was able to show fabrication of evidence, upon which the individual then admitted wrongdoing in a deposition. The individual was then sanctioned.

CASE STUDY 25: FORMER MANAGER

A manager of a Big 10 consulting firm went to work for a competitor. Under court order, the competitor provided a diskette that had gone with the individual to the new firm. A computer forensics team was hired to inspect said diskette. Although it was damaged, deleted, and overwritten, evidence of illegal customer lists and the lists themselves were discovered on the diskette.

E Answers to Review Questions and Exercises, Hands-on Projects, Case Projects, and Optional Team Case Projects by Chapter

PART I: OVERVIEW OF COMPUTER FORENSICS TECHNOLOGY

Chapter 1: Computer Forensics Fundamentals

Review Questions and Exercises

True/False

1. True
2. False
3. True
4. True
5. True

Multiple Choice

1. B
2. A
3. E
4. D
5. E

Exercise

The following is a partial solution to aide the computer forensics specialist (CFS) in coming up with his or her own solution to solve this case. Applying forensic data analysis methods, the CFS downloaded five years worth of general ledger data from a mainframe computer system, along with large volumes of data from client file servers. Digital data preservation, coupled with data mining and analysis, confirmed the extent of fraudulent activity and allowed the company to correct its public record filings about its financial worth.

Hands-on Projects

Your computer forensics team would provide on-site computer forensic evidence preservation, digital evidence recovery, file inventory, and data analysis. Data would be sent to an advanced document management services center (DMSC) for the hosting and support of attorney document and email review. The DMSC would provide advanced document management services for capturing, storing, retrieving, analyzing, viewing, and sharing discovery information and work product. By providing your own tools for discovery collaboration, you can help reduce your costs and your risks. Most DMSCs are housed in a highly secure 40,000+ square foot facility, and staffed by systems and network engineers, database designers, software developers, litigation support personnel, and industry-focused professionals.

Case Project

The boss instructs the sysadmin to take immediate steps to preserve the collected packets. He then contacts the company's chief information security officer (CISO) and informs him of the situation. The CISO recognizes this as a security incident that could compromise the company's proprietary information and trade secrets; it could also involve the employee whose workstation contacted the competition's IP address. Fortunately, this is exactly the kind of incident the company had in mind when it developed the computer forensic annex to its information security plan.

The CISO assigns an incident manager from his organization to oversee the event. The incident manager then contacts the company's general counsel to discuss the various legal issues involved in the investigation. Next, he calls out a forensics technician to collect and preserve the evidence from the sysadmin's computer, the employee's workstation, the database server, and the firewall.

After conducting a routine examination of the collected material, the forensic technician notices a substantial amount of proprietary information on the employee's hard drive that he does not appear to need. Moreover, the forensic technician can't identify the mechanism used to communicate with the competitor's computer. Analysis of the server and firewall logs reveals that lots of information was transferred from the database server to the competition.

After obtaining the general counsel's approval, the incident manager engages a researcher at a major university to review the examination results and work product. The researcher identifies code on both the employee workstation and the database server that's written to send information from the database server to the competitor's computer on command from the employee's workstation.

This command is determined to be the first and middle name of the employee's oldest daughter. The incident manager uses the reports from the forensic technician and the researcher to write an incident report for executive management. On the basis of this incident report, the employee confesses to cooperating with an associate employed by the competition. The general counsel sues the competitor for damages, obtaining a restraining order against the competition and demonstrating the company's aggressive protection of its trade secrets.

Optional Team Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. You should deploy CFSs to the client locations worldwide to preserve electronic evidence. The team should search through the electronic data and provide an onsite delivery strategy for legal review, thus allowing the client to expeditiously comply with the SEC requirements.

Chapter 2: Types of Computer Forensics Technology

Review Questions and Exercises

True/False

1. False
2. True
3. False
4. False
5. True

Multiple Choice

1. C
2. D
3. E, A
4. E
5. E, B

Exercise

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. Through DMSC's remote access and electronic data mapping tools, the review team was reduced to six people working from their remote offices, thus eliminating unnecessary travel costs, and the review time was reduced by 82%. The client ultimately saved approximately $5.69 million in review and travel costs while identifying key documents and correspondence for additional follow-up.

Hands-on Projects

The following is a partial solution to aide the CFS in coming up with his or her own solution to solve this case. The accounting firm's computer forensics team collected electronic and hard copy evidence that contributed to an extra-judicial confession revealing that the employee had embezzled a material sum over a four-month period. They also identified programmatic and systemic internal control weaknesses that would have allowed other employees to engage in similar embezzlement schemes without detection.

Case Project

This case project is a blending of a number of incidents examined in the latter part of 2004 and doesn't represent any single incident. However, all of the incidents observed shared certain common traits: large enterprises supported by extremely high bandwidth Internet connections, largely Windows NT and Windows 2003 enterprises, persistent compromise of administrator and domain administrator accounts, and widespread use of a distributed two-tier FTP server—where the FTP root directory structure was composed of a virtual file system of shared drives. The fictitious company, WebFile.com, suffers from this same set of common criteria, and like most of the real-world incidents, the attackers are serving both warez and porn.

At this stage of the investigation, the CFS has discovered the compromise (although the CFS has yet to identify the compromise method), identified the post-attack "fingerprint" of this particular group, and has begun to understand what is happening in the enterprise. Should the CFS need to initiate corrective action at this time, there are a number of things he or she can do to end the current compromise, starting with changing the administrator passwords, and restricting NetBIOS using packet filters on the switches supporting the WebFile.com enterprise. However, before the CFS starts with the eradication phase of the incident response, he or she really needs to complete the identification phase: the CFS has yet to identify the initial compromise method or to identify the scope of the compromise. In the optional team case project, the CFS will look at network traffic analysis techniques to continue his or her response and resolve these issues.

Optional Team Case Project

The network side of the analysis is often much more time consuming than the "live approach" of a compromised host. As a CFS, you have to learn to discriminate between normal traffic and the traffic you believe to be abnormal and possibly malicious. In the preceding case project, the CFS had the home-field advantage over the attackers. After reading the numerous emails the CFS has received from the field, it may be more accurate to say that the CFS *ought* to have the home-field advantage. The CFS ought to know the policies networks operate under, and those policies ought to be complied with. While this is not always the case in reality, it is certainly something the CFS ought to strive for.

Historically, the Windows environment has been difficult to monitor, analyze, and secure, simply because of the lack of security tools that run on the platform. The astute reader will note that this is the possible source of the original compromise but cannot conclusively prove it. The reality of the situation is that this sometimes happens, particularly in complex environments where there is poor access control and monitoring. Some data sources are usually not investigated, such as the Windows Event and Security Logs, Web server logs, etc. In a real incident these should absolutely be studied. Often there is sufficient data in the enterprise to rule out certain kinds of attacks even if a robust network security monitoring environment isn't in place.

In this optional team case project, several "cardinal rules" of security were violated. The batch file would not have operated successfully as written if the administrator account was not identical on each host. The global domain administrator account was actually the same as each local administrator account, further reducing the security of the enterprise as a whole. The second major problem was the bad monitoring environment. Clearly some architectural changes and a redesign of the network are called for. By using some of the tools with minimal cost, it is possible to build a rudimentary intrusion detection system (IDS) capability, although monitoring it will probably take significant manpower.

At the risk of starting a religious discussion, Windows is neither more nor less inherently secure than any other platform—with a few arguable exceptions. It is one of the most attacked operating systems on the face of the planet, thanks to its wide proliferation. As a result, its flaws are exploited often and well. If you are running a large Windows environment, my advice is to prepare yourself for the inevitable compromise by doing the following:

- Build a toolkit.
- Characterize the network.
- Implement an IDS—even a rudimentary one.

Finally, take the time to prepare yourself. This goes beyond characterizing the environment, although that's a good first step. Most importantly, take the time to dig into the tools and practice using them. Learn their features and filter languages in particular, as these will be infinitely useful to you the more you learn.

Chapter 3: Types of Computer Forensics Systems

Review Questions and Exercises

True/False

1. True
2. False
3. False
4. True
5. True

Multiple Choice

1. D
2. E
3. B
4. A, E
5. C, D

Exercise

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. Further analysis of all accounts held by Larry is performed by the forensics system. In addition to the ATM cash withdrawal, an Internet banking transfer to an overseas account has also been made. The system creates an alert and escalates to bank security staff for follow-up.

Hands-on Projects

At 11:37 A.M., the forensics system issues an alert to the enterprise computer forensics team, who investigate the incidents. They discover that a person posing as a computer technician advised other staff on the two floors that he had to perform service work on the two PCs. With no obvious evidence of tampering with the PC, the computer forensics team call in another staff member to perform a sweep of both offices for hidden audio recording units. Such are found in both offices, and at 12:56 P.M., the police are notified of the incident.

Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. The CFS escalates the incident to a bank security officer to contact Karin by telephone to determine the validity of the Internet banking transaction. It is discovered that the Internet banking transaction is fraudulent. The bank's CFS instructs the forensics system to analyze all transactions related to IP addresses from Turin, Italy, and discovers another 39 suspect transactions.

Optional Team Case Project

The organization's computer forensic technology team uncovered digital evidence of a false invoicing scheme perpetrated by the executive and vendor coconspirators over a six-year period, resulting in a major embezzlement of corporate funds. Analysis of digital and other evidence traced the flow of embezzled funds through an elaborate interstate money-laundering scheme. The investigation resulted in a referral to the FBI and the subsequent indictment of the senior executive.

Chapter 4: Vendor and Computer Forensics Services

Review Questions and Exercises

True/False

1. False
2. True
3. False
4. True
5. True

Multiple Choice

1. A
2. C
3. C
4. E
5. B

Exercise

The CFS identified numerous email messages that exposed the company to sexual harassment lawsuits. The CFS also recovered emails between management officials and outside auditors that called into question an auditor's independence. The CFS advised the company to establish a digital information destruction policy, create an equal employment opportunity (EEO) and sexual harassment training program, implement a computer and Internet usage policy, educate employees about the new policies, and monitor compliance.

Hands-on Projects

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. With help from the CFS team (CFST), a high-quality large-format imaging firm recently won its case against two former employees. The CFST was able to recover the email and the database for the imaging firm and subsequently testified to the findings of their forensic analysis. The former employees lost their credibility and the case.

Case Project

In the preliminary stages of an employment dispute case, a CFST was brought in by a large computer services corporation to perform a forensic recovery on an employee's desktop computer. After performing a forensic analysis, the CFST could find no evidence of hacking on the employee's computer. Thus, the employee was exonerated of any wrong-doing and other costly proceedings were averted.

Optional Team Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. A CFS team was hired to locate any deleted files and verify certain illicit and non-work related contents of the hard drives in question. Forensic technicians were able to locate spy software, illegal file-sharing software, pornography, and information pertaining to a personal side business. Both the CEO and the network administrator were dismissed as a result of the investigation.

PART II: COMPUTER FORENSICS EVIDENCE AND CAPTURE

Chapter 5: Data Recovery

Review Questions and Exercises

True/False

1. False
2. False
3. False
4. False
5. False

Multiple Choice

1. C
2. E, B
3. E, A
4. B
5. D

Exercise

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. The CFS received three backup tapes and the hard drive from the system. Within 48 hours, the CFS had successfully recovered 100% of the data believed to have been lost in the fire.

Hands-on Projects

The CFST was able to restructure and reformat all the files needed for the claimant's specific software application and reprogram data. Using electronic data discovery and forensic and analysis applications, the CFST discovered that the software installation had not caused the data loss and determined the plaintiff had manually erased the alleged lost data. When shown the evidence, the plaintiff dropped the suit and was promptly countersued.

Case Projects

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. Within three days, the CFST was able to recover 100% of the data from four of the drives; 99% was recovered from the fifth drive.

Optional Team Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. By using the password encryption proprietary program and programming knowledge of the email system, the CFST was able to locate all emails and attachments meeting selected criteria and electronically transmitted them to the court within only five days. The case was settled in the plaintiff's favor on the seventh day. The defendant was charged with perjury.

Chapter 6: Evidence Collection and Data Seizure

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. False
5. False

Multiple Choice

1. D
2. A
3. A
4. C
5. E

Exercise

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. During the research of her computer, the CFS was able to recover several deleted email messages exchanged between the young girl and a suspect. These emails led police to a nearby motel where the girl was located and the adult male was taken into custody.

Hands-on Projects

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. A trained CFS was able to establish a timeline of Internet activity indicating visits to several Web sites deemed inappropriate by the parents.

Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. After an investigation, a forensics specialist determined that the accused roommate did indeed make the purchases and had altered the computer's time clock in an attempt to hide his activity.

Optional Team Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. A CFS was able to recover several profane emails sent by the plaintiff's boss to another supervisor planning ways to "get rid" of her. The case was settled before trial.

Chapter 7: Duplication and Preservation of Digital Evidence

Review Questions and Exercises

True/False

1. False
2. False
3. False
4. True
5. False

Multiple Choice

1. A, B
2. C
3. D, A
4. D
5. A

Exercise

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. A CFST was engaged to copy and archive each workstation computer hard drive for future analysis in case a dispute over intellectual property arose in the future.

Hands-on Projects

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. A CFS working alongside the network administrator proved that the accused employee did not download the images, but in fact the images were "planted" there across the network by another disgruntled employee. When confronted with the evidence, the disgruntled employee admitted to the incident and left employment with the company. The wrongly accused employee is also suing the employee who planted the images.

Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. CFS analysis produced evidence of ties to other crimes and suspects including car theft, prostitution, firearms violation, and identity theft. Ultimately 28 arrests were made, yielding 23 felony convictions.

Optional Team Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. The findings revealed over $20,000 of missing revenue in the previous 19 months. Once confronted with this information, the bookkeeper admitted to the crime and was forced to make restitution.

Chapter 8: Computer Image Verification and Authentication

Review Questions and Exercises

True/False

1. False
2. False
3. True
4. False
5. False

Multiple Choice

1. C, B
2. D
3. B
4. B
5. B

Exercise

To narrow the scope of meaningful data, the CFST used forensics utilities to search for relevance and responsiveness—a necessity in a discovery request of this magnitude under the given time constraints. This enabled the CFST to better focus their tape conversion efforts. Using further forensics processes, they converted the company's Microsoft Exchange database (which housed the company's email archives, the focus of the discovery efforts) to

PST files, sorted by user. The CFST was thus able to help the company meet its seemingly impossible deadline. The CFST continued conducting an ongoing analysis to keep the company in compliance with the discovery mandate.

Hands-on Projects

Initially, the CFST was requested to perform forensics examinations upon scores of the publicly owned company's computers from locations around the world—a service that would easily add up to over $200,000 in initial consulting services. Working with the accounting firm and the company, the CFST convinced both parties to significantly narrow the universe of computers to be searched; the conjecture was that given the parameters of the matter, any trail of malfeasance would likely lead to the executive ranks. The accounting firm and client agreed. Initial processing has revealed several key leads for a fraction of the initial projected expense. The matter is ongoing.

Case Project

A mirror image backup of the laptop's hard drive was made, and a forensic examination was conducted. The CFST obtained a listing of all deleted and undeleted files from the mirror image backup and performed a search for key words associated with the sensitive files suspected of being downloaded. It was proved that certain sensitive files had been on the laptop's hard drive. A file listing time-line analysis was performed, and it showed that numerous files were loaded on the computer while the employee was on leave of absence and the laptop computer was in his possession. A network log check was also performed with the help of the bank's computer systems staff. This showed that the employee had been logged onto the network during the times that the questioned files first appeared on the laptop. Thanks to the evidence gathered and leads developed during the CFTS's examination, the bank referred the case to the FBI for criminal investigation.

Optional Team Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. After making a mirror image backup of the ex-boss' hard drive, the CFST was able to recover deleted electronic messages that showed that the ex-boss had a history of propositioning women under his supervision for "special favors." A situation that might have been mired in a "he said/she said" continuum was quickly resolved; the woman got her job back (including all lost wages and benefits), and the real culprit was terminated.

PART III: COMPUTER FORENSICS ANALYSIS

Chapter 9: Discovery of Electronic Evidence

Review Questions and Exercises

True/False

1. True
2. False
3. False
4. False
5. False

Multiple Choice

1. E
2. D
3. B
4. A, B
5. C, D

Exercise

No evidence could be found that the second angiogram images had ever been stored on the computers, or that the images had been deleted. Through inquiries of hospital staff, the CFST learned that the system was prone to problems and periodically "crashed." The CFST requested that the hospital perform a test case on the system, and it was observed that the system malfunctioned; in the test case, no images were recorded. Subsequently, the hospital replaced this system with a new system because of the periodic crashes that occurred. A CFST examiner testified at the jury trial that system crashes may have caused the images to not be stored on the computer hard drives and that he had personally observed the system crashing. The plaintiff's attorneys countered that the manufacturer examined the system the day after the patient's death and could not find any problems. The CFST's examiner countered that the system had been replaced by the hospital because of system malfunctions. He further explained that because the system was functioning normally on the day the manufacturer examined the system, did not mean that it was functioning on the day of the second angiogram procedure. The best outcome that the insurance company expected was elimination of any penalties for deliberate deletion of the images. The jury ruled that no monetary damages would have to be paid to the plaintiffs. The attorney for the insurance company later stated, "Your investigation and testimony played a significant role in our presentation of the case to the jury ... all of the feedback from the jurors has been extremely positive toward you and your testimony."

Hands-on Projects

After making mirror image backups of the hard drives, the CFST identified a file directory that had been deleted during the aforementioned four-day period that had the same name as the competitive company the executive had established. A specific search of the deleted files in this directory identified the executive's "to do list" file. This file indicated that the executive planned to copy the company's database (valued at $100 million) for his personal use. Another "to do" item specified that the executive was to "learn how to destroy evidence on a computer." The CFST's examination also proved that the executive had been communicating with other competing companies to establish alliances, in violation of the executive's nondisclosure agreement with the company. It was also shown that numerous key company files were located on removable computer storage media that had not been turned over by the executive to the company. The company was able to settle with the executive for all that it had originally requested in its lawsuit.

Case Project

The entire acquisition occurred without the knowledge of anyone in Asia and without disrupting operations. The investigation also revealed that the other drive did not contain relevant evidence. The computer forensic tool essentially enabled an investigation that otherwise would likely not have taken place. An investigation involving international travel, flyaway kits, and stand-alone computer forensics utilities would have delayed the process by several days, if not weeks, thus resulting in altered data or loss of evidence. An on-site response process may have comprised the investigation in this case or, at a minimum, impacted business and morale because of the very non-clandestine physical presence of investigators.

Optional Team Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. A large government agency used a CFST's computer forensic tool and a high-speed network connection to image a drive on its wide area network (WAN) located approximately 10,000 miles (16,000 km) away. This process enabled a rapid incident response and the capturing of the data. Without the CFST's computer forensic tool, the response would have been delayed by several days or may not have occurred.

Chapter 10: Identification of Data

Review Questions and Exercises

True/False

1. True
2. True
3. True
4. True
5. True

Multiple Choice

1. A
2. A, B
3. D, E
4. C
5. A

Exercise

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. The CFST successfully used a computer forensics tool to preview the server and collect key evidence, without disrupting operations. Without the computer forensics tool, the CFST would have either walked away from the scene empty-handed or performed a highly invasive and incomplete investigation by making logical file copies of active data.

Hands-on Projects

The CFST used a computer forensics tool and network logs to examine the files on 60 network machines. The CFST determined that large amounts of pornography were traveling through the network. It was discovered that unauthorized Web servers containing more than 20 gigabytes of pornographic material had been set up across the network. Using computer forensics tool, they were able to determine which users had access privileges and had logged onto the suspected machines. An unexpected result of the investigation revealed additional rogue servers placed above ceiling tiles, communicating with the network via multiple wireless access points. In a weekend, enough evidence was gathered to determine that the entire network administration team had been part of a sophisticated porn operation. The whole team was immediately terminated. By using the CFST, the entire investigation was performed in only 2 days—10 days fewer than expected. The result was significant timesaving and reduced investigative fees. In addition, the company had sufficient evidence to protect itself from a wrongful termination suit. The porn operation was shut down and the corporate bandwidth returned to normal, and the company prevented a huge possible liability.

Case Project

The CFST was used to perform an exhaustive search of all computer records within the company's large finance division. It was soon discovered that management ordered staff to destroy key documents. However, certain staff members did not fully comply with the order, making the files easily recoverable. In addition, on some systems, the CFST was able to recover incriminating documents that had been deleted. The entire process occurred without affecting business operations or productivity. Eventually, enough information was recovered to reconstruct the actual events and prove that numerous high-level managers had schemed to alter the records of the company. The suspected staff members were terminated and criminal charges were brought against them.

Optional Team Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. Using a combination of forensic analysis of the hard drives and investigation (tracing IP addresses, etc.), the CFST was able to identify the hacker, which would enable law enforcement to obtain a search warrant if the client elected to press charges.

Chapter 11: Reconstructing Past Events

Review Questions and Exercises

True/False

1. True
2. False
3. True
4. False
5. True

Multiple Choice

1. B
2. B
3. E
4. E
5. A

Exercise

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. Using forensic analysis, the CFST determined that the documents had been created and printed out, but never saved on the desktop computer at one of the workstations utilized by one of the four suspects.

Hands-on Projects

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. The CFST's analysis revealed that the paralegal had in fact created the document weeks prior to the deadline, and the file had not been accessed or altered. The CFST appeared as expert witnesses at the hearing, which resulted in a favorable ruling for the client when the judge set aside the default judgment and re-opened the case.

Case Project

The following is a partial solution to aid the CFS in coming up with his or her own solution to solve this case. No evidence of the theft was found, but significant evidence of other activities (for which he could be terminated) was found.

Optional Team Case Project

The CFST forensically preserved all of the evidence of the attacks and the harassing email. Given the potential for violence, the CFST posted armed security at its clients' offices. After tracing the origin of one of the harassing emails to the fired developer's new place of employment, the CFST enlisted the cooperation of the new employer, which resulted in the forensic imaging of the developer's new laptop. Found on the hard drive was cached information showing that the developer had used the laptop to transfer the stolen compensation information. The CFST presented this information and results of its internal investigation to the U.S. Secret Service and the U.S. Attorney's Office in Manhattan, which accepted prosecution. The developer was arrested, his home was searched (leading to the recovery of hardware stolen from the CFST's client), and he was placed under strict bail conditions to protect the frightened clerk.

Chapter 12: Networks

Review Questions and Exercises

True/False

1. False
2. True
3. False
4. True
5. False

Multiple Choice

1. D, E
2. C
3. A
4. A
5. B

Exercise

In the course of the engagement, the CFST imaged seven desktop and server hard drives and performed forensic analysis. The CFST also constructed Lotus Notes and Microsoft Outlook test environments to explore arcane issues relating to extended simple mail transfer protocol (ESMTP) timestamping and the generation of Lotus Notes message identification numbers. Using the results of the forensic analysis (including significant data recovered from deleted file space) and the information generated from the test environments, the CFST was able to reach expert conclusions regarding the authenticity of the different versions of this critical email.

Hands-on Projects

The CFST provided the executive with critical advice regarding whether to involve law enforcement, explaining in detail how the process would work, dispelling incorrect notions, and helping resolve conflict within the client's management regarding a criminal referral. The CFST introduced the client to trusted former colleagues at the FBI and acted as liaison. Carrying out the executive's clear mandate to bring the hackers to justice, the CFST assisted the FBI in developing and executing an undercover plan to lure the hackers to a Western country for a face-to-face meeting. The CFST worked closely with the law enforcement authorities in that foreign country. Through its actions and advice, the CFST provided its client with incomparable comfort that decisions were being made properly, that safety was insured, that the plan would be effective, and that the client still had a large degree of control over the situation. The CFST arranged for its client to travel to that Western country, where—after a face-to-face meeting in an undercover law enforcement location—the hackers were arrested on extortion charges. The CFST later provided substantial liaison with the FBI, even providing the forensic evidence needed to extradite the hackers back to the United States.

Case Project

Within hours, the CFST had NT systems experts working closely with the company's IT personnel. Using utilities to perform macro-by-macro and line-by-line comparisons between backups and the improperly accessed databases, the CFST was able to deliver good news to the company: the production databases had in fact not been corrupted, contrary to what the firewall logs had initially indicated. The CFST also found serious weaknesses in the company's logging system. In fact, these weaknesses made it impossible to identify all of the servers that the intruder accessed. As a result, the company needed to decide whether to incur the cost of a server-by-server search for potentially corrupted files. Based upon an analysis of the intruder's skill level and behavior, the CFST was able to offer the company the guidance it needed to make that decision. For the company, a complex decision remained—whether to proceed criminally or civilly against the ex-employee. Knowing the law enforcement and legal options, each path opened up and closed off, the CFST clarified important elements, including which path would give the bank the most control and which path would most likely provide access to the ex-employee's home computer—something that would fill in damage assessment gaps created by the weaknesses in the bank's logging system. Crucial to the company's decision was the fact that the CFST had uncovered and preserved significant forensic evidence linking the ex-employee with the computer break-in. Ultimately, this evidence was used to support a successful application for a temporary restraining order against the ex-employee.

Optional Team Case Project

Working closely with the firm's systems administrators, the CFST quickly captured the IP address used in one of the attacks. After then guiding the firm through the factors involved in making a criminal referral, the CFST referred the case to former colleagues at the U.S. Attorney's Office for the Western District of Los Angeles and the U.S. Secret Service. Within hours, the Secret Service had linked the captured IP address to a computer in the library of the employee's college, located a witness at the library, and identified files belonging to the employee on the relevant computer's hard drive. The employee was arrested, detained without bail, and later indicted. He subsequently pleaded guilty to launching the attacks in violation of the Computer Fraud and Abuse Act. Once the suspect was in custody, the CFST focused on making sure he would pose no future threat. The CFST assessed the dollar value of the loss suffered by the firm, knowing that the assessment would prove critical in the calculation of the employee's sentence, in this case an eight-month prison term.

PART IV: COUNTERMEASURES: INFORMATION WARFARE

Chapter 13: Fighting Against Macro Threats: Defensive Strategies for Governments and Industry Groups

Review Questions and Exercises

True/False

1. False
2. True
3. True
4. True
5. True

Multiple Choice

1. B
2. A
3. E
4. D
5. E

Exercise

Initially, the CFS was requested to perform forensics examinations upon scores of the publicly owned company's computers from locations around the world—a service that would easily add up to over $400,000 in initial consulting services. Working with the accounting firm and the company, the CFS convinced both parties to significantly narrow the universe of computers to be searched; the conjecture was that given the parameters of the matter, any trail of malfeasance would likely lead to the executive ranks. The accounting firm and client agreed. Initial processing revealed several key leads for a fraction of the initial projected expense.

Hands-on Projects

A forensic image backup of the laptop's hard drive was made, and an examination was conducted. The CFST obtained a listing of all deleted and undeleted files from the mirror image backup and performed a search for key words associated with the sensitive files suspected of being downloaded. It was proved that certain sensitive files had been on the laptop's hard drive. A file listing timeline analysis was performed, and it showed that numerous files were loaded on the computer while the employee was on leave of absence and the laptop computer was in his possession. A network log check was also performed with the help of the bank's computer systems staff. This showed that the employee had been logged onto the network during the times that the questioned files first appeared on the laptop. Thanks to the evidence gathered and leads developed during the CFST's examination, the bank referred the case to the FBI for criminal investigation.

Case Project

The hard drive from the executive's notebook and desktop machine were forensically imaged. The CFS's analysis established that the night before the executive left, he downloaded all of the company's process specifications and distributor agreements, which he then zipped and emailed via dial-up ISP to the competitor he would be joining. Additionally, reconstruction of deleted files located emails between the executive and the competitor discussing his intent to provide the proprietary information if he was offered additional options in the new company.

Optional Team Case Project

A CFST was retained by the plaintiff's attorneys to investigate allegations of the former supervisor's harassing behavior. After making a forensic image backup of the ex-boss' hard drive, the CFST was able to recover deleted electronic messages that showed that the ex-boss had a history of propositioning women under his supervision for "special favors." A situation that might have been mired in a "he said/she said" continuum was quickly resolved; the woman got her job back, and the real culprit was terminated.

Chapter 14: The Information Warfare Arsenal and Tactics of the Military

Review Questions and Exercises

True/False

1. False
2. False
3. False
4. True
5. True

Multiple Choice

1. B
2. E
3. A
4. B
5. C

Exercise

After making a forensic image backup of the hard drives, the CFST identified a file directory that had been deleted during the aforementioned five-day period that had the same name as the competitive company the executive had established. A specific search of the deleted files in this directory identified the executive's "to do list" file. This file indicated that the executive planned to copy the company's database (valued at $400 million) for his personal use. Another "to do" item specified that the executive was to "learn how to destroy evidence on a computer." The CFST's examination also proved that the executive had been communicating with other competing companies to establish alliances, in violation of the executive's nondisclosure agreement with the company. It was also shown that numerous key company files were located on removable computer storage media that the executive had not turned over to the company. The company was able to settle with the executive for all that it had originally requested in its lawsuit.

Hands-on Projects

The investigation of Internet use and traffic pinpointed a clash of IP addresses on the system. The evidence started to point toward the organization's system administrator, but he denied it. The CFS proved that it was the administrator who'd been using his local desktop system to access numerous pornographic Web sites. Over three months, he had visited 4,500 pornographic Web sites and downloaded over 48,000 images. To cover his tracks, and in an attempt to frame a senior manager, he had been altering his local system IP address so the trail led to his senior manager colleague. The expertise in computer forensics and incident response saved an innocent person's job and good name and uncovered the real culprit. The senior manager was cleared of all involvement, and his reputation was restored.

Case Project

A CFST was asked to examine the departing manager's personal laptop computer to determine if the individual in question had been negotiating in bad faith. The CFST was able to extract evidence from the laptop drive that:

- The individual in question had negotiated in bad faith and had never intended to stay with the CFST's client's company.
- The individual had negotiated the contract with the full intention of resigning immediately on signing.
- The individual had repeatedly over a period of months passed highly sensitive information to his former colleagues in the competing company.
- The individual had been a director of the competing company even prior to the original buy-out.
- The individual had been involved in the day-to-day management of the competing company.
- The individual had been involved in the defection of key staff from the CFST's client to the new company.
- The individual had conspired with other employees of the subsidiary to mismanage it, leaving the market open to the new company.

- The individual had used company resources to research and solicit the services of escorts.
- The individual has used his computer to store and manage a large quantity of homemade pornographic imagery.

Court action was initiated to prevent the transfer of $40 million to the individual responsible. Court action was initiated against the individual and others for breach of contract and fraud.

Optional Team Case Project

A CFST was able to confirm the extensive damage to the casing and motherboard of the computer, but the hard disk was undamaged and the forensic company recovered all the data from it, thus saving the insurance company from a fraudulent claim.

Chapter 15: The Information Warfare Arsenal and Tactics of Terrorists and Rogues

Review Questions and Exercises

True/False

1. False
2. True
3. True
4. False
5. False

Multiple Choice

1. A
2. A
3. D
4. E
5. D

Exercise

Using a combination of forensic analysis of the hard drives and investigation (tracing IP addresses, etc.), a CFS was able to identify the hacker, which would enable law enforcement to obtain a search warrant if the client elected to press charges.

Hands-on Projects

Within 48 hours, the CFST had successfully recovered 100% of the data that the company thought they had lost in the fire.

Case Project

Using advanced data forensic recovery, the CFS was able to recover 9 million emails within five days. Within five days of obtaining the tapes, working a normal eight-hour day, the CFS had located 9.5 million emails on the November and December 2004 tapes. Because of time pressure, the parties agreed that the plaintiff would produce all of the 4 million emails that the CFS had been able to print out. This strengthens the claim that off-the-shelf recovery and e-evidence discovery tools are not the most advanced way to recover data. In addition, the forensic investigator will most likely benefit from and be able to prepare a better case when employing advanced recovery services. The courts are beginning to recognize this and that better, more advanced technology exists. Furthermore, not using the available technology can lead to sanctions.

Optional Team Case Project

The CFS was able to recover the email and the database for the format imaging firm and subsequently testified to the findings of their forensic analysis. The defendants lost their credibility and the case. After a four-week trial, a San Antonio, Texas, jury rendered a $2.98 million verdict in favor of the format imaging firm. The jury of seven women and five men heard the evidence in two phases. In the first phase, among other things, the jury found that the format imaging firm's former general manager breached his fiduciary duties, misappropriated trade secrets, and engaged in fraud. In the second phase, the jury found that the defendants acted with malice. Many lawyers, judges and even would-be criminals incorrectly assume that deleted or corrupted files are irretrievable. However, with the forensic technology that's available today, no computer crime can go unsolved.

Chapter 16: The Information Warfare Arsenal and Tactics of Private Companies

Review Questions and Exercises

True/False

1. True
2. False
3. True
4. False
5. True

Multiple Choice

1. C
2. B
3. A
4. D
5. A

Exercise

After performing a forensic analysis, the CFS could find no evidence of hacking on the employee's computer. Thus, the employee was exonerated of any wrong-doing, and other costly proceedings were averted.

Hands-on Projects

The CFST was able to locate spy software, illegal file-sharing software, pornography, and information pertaining to a personal side business. Both the CEO and the network administrator were dismissed as a result of the investigation.

Case Project

The CFS was able to restructure and reformat all the files needed for the claimant's specific software application and reprogram data. By using electronic data discovery and forensic and analysis applications, the CFS discovered that the software installation had not caused the data loss and determined that the plaintiff had manually erased the alleged lost data. When shown the evidence, the plaintiff dropped the suit and was promptly countersued.

Optional Team Case Project

Within four days, the CFS was able to recover 100% of the data from four of the drives; 99% was recovered from the fifth drive.

Chapter 17: Information Warfare: Arsenal of the Future

Review Questions and Exercises

True/False

1. False
2. False
3. False
4. True
5. True

Multiple Choice

1. B
2. B
3. A
4. C
5. A

Exercise

Using a password encryption proprietary program and programming knowledge of the email system, the CFS was able to locate all emails and attachments meeting selected criteria and electronically transmitted them to the court within only four days. The case was settled in the plaintiff's favor on the eighth day. The defendant was charged with perjury.

Hands-on Projects

The entire acquisition occurred without the knowledge of anyone in Asia and without disrupting operations. The investigation also revealed that the other drive did not contain relevant evidence. The CFST essentially enabled an investigation that otherwise would likely not have taken place. An investigation involving international travel, flyaway kits, and stand-alone computer forensics utilities would have delayed the process by several days, if not weeks, thus resulting in altered data or loss of evidence. An on-site response process may have compromised the investigation in this case or, at a minimum, impacted business and morale because of the very non-clandestine physical presence of investigators.

Case Project

This process enabled a rapid incident response and the capturing of live data. Without the CFS, the response would have been delayed by several days or may not have occurred.

Optional Team Case Project

The CFS successfully previewed the server and collected key evidence, without disrupting operations. Without the CFS, law enforcement investigators would have either walked away from the scene empty-handed or performed a highly invasive and incomplete investigation by making logical file copies of active data.

Chapter 18: Surveillance Tools for Information Warfare of the Future

Review Questions and Exercises

True/False

1. True
2. True
3. True
4. True
5. True

Multiple Choice

1. C
2. B
3. A
4. D
5. A

Exercise

Network logs and the files on 60 network machines were examined. The CFST determined that large amounts of pornography were traveling through the network. It was discovered that unauthorized Web servers containing more than 30 gigabytes of pornographic material had been set up across the network. The CFST was able to determine which users had access privileges and had logged onto the suspected machines. An unexpected result of the investigation revealed additional rogue servers placed above ceiling tiles, communicating with the network via multiple wireless access points. In a weekend, enough evidence was gathered to determine that the entire network administration team had been part of a sophisticated porn operation. The whole team was immediately terminated. The CFST performed the entire investigation in only 3 days; 11 days fewer than expected. The result was significant timesaving and reduced investigative fees. In addition, the company had sufficient evidence to protect itself from a wrongful termination suit. The porn operation was shut down and the corporate bandwidth returned to normal, and the company prevented a huge possible liability.

Hands-on Projects

The CFS performed an exhaustive search of all computer records within the company's large finance division. It was soon discovered that management ordered staff to destroy key documents. However, certain staff members did not fully comply with the order, making the files easily recoverable. In addition, on some systems, the CFS was able to recover incriminating documents that had been deleted. The entire process occurred without affecting business operations or productivity. Eventually, enough information was recovered to reconstruct the actual events and prove that numerous high-level managers had schemed to alter the records of the company. The suspected staff members were terminated and criminal charges were brought against them.

Case Project

The CFST was able to reveal nearly 16 million U.S. dollars worth of Central Excise duty evasions. Handling the audit, the CFST was also able to identify crucial evidence that resulted in the safeguarding of 7.6 million U.S. dollars of government revenue. The data retrieved by the CFST exposed a central duty evasion scheme that had robbed the Indian government of 2.5 million in U.S. dollars. In exposing false claims and fabricated documents, the CFST was able to provide analysis and information in the case that supported the seizure of cash, equivalent to $435,000. The CFST was also able to quickly analyze dozens of hard drives and sift through voluminous amounts of evidence against plywood manufacturing companies based in India. The examination uncovered five years' worth of unaccounted transactions. The resulting data provided a critical foundation for further investigation by India's Central Excise Intelligence Department. The incident exposed an evasion of excise duties totaling nearly 5.4 million in U.S. dollars. Qualitatively and quantitatively, the outputs provided by the CFST were an invaluable contribution to the interests of government revenue.

Optional Team Case Project

APD did have the authority from the court to seize the server in this case. They were able to secure the scene, and the CFS called the system administrator and requested administrative access to the server. The CFS knew he could do the acquisition on scene and offered the company the ability to cooperate with the APD while the he conducted the investigation in the least intrusive manner available. If the company didn't agree to the CFS having system access, APD would have had the authority to seize the hardware, and any loss of productivity or data would have been their own responsibility. After having received access to the company's system, the CFS was able to conduct a live acquisition using a portable forensic computer plugged into an available port on a 36-port switch. The CFS ended up downloading two 33.6 SCSI drives full of data. The CFS had brought with him enough target media for 720 gigabytes worth of data. The CFS then walked onto the scene with six 120-gigabyte drives not knowing what to expect. The CFS seized the workstations and conducted the acquisition of these computers back at the APD, where he had the ability to do four acquisitions at a time. APD executed the search warrant at 7:00 A.M. on Monday morning and had every system processed, reinstalled, and up again by noon on Wednesday. In two and a half days, the CFS had that business back up and running. The CFS is now working on the analysis after having conducted a triage of the emails. If it wasn't for the CFS's speed and efficiency and availability to acquire data through a network, the city of Austin would be looking at a huge liability. APD did everything possible to limit that company's loss of productivity. Basically, APD conducted the data seizure in a manner that was in the best interest of the city and this company. Interestingly enough, on that Wednesday afternoon the, case agent called the CFS and said that the company's attorney was demanding that APD return their computers immediately. The CFS told him that the computers had already been returned and had been up and running in their business since noon.

Chapter 19: Civilian Casualties: The Victims and Refugees of Information Warfare

Review Questions and Exercises

True/False

1. False
2. False
3. False
4. False
5. False

Multiple Choice

1. C
2. A
3. B
4. C
5. D

Exercise

Network logs and the files on 60 network machines were examined. The CFST determined that large amounts of pornography were traveling through the network. It was discovered that unauthorized Web servers containing more than 30 gigabytes of pornographic material had been set up across the network. The CFST was able to determine which users had access privileges and had logged onto the suspected machines. An unexpected result of the investigation revealed additional rogue servers placed above ceiling tiles, communicating with the network via multiple wireless access points. In a weekend, enough evidence was gathered to determine that the entire network administration team had been part of a sophisticated porn operation. The whole team was immediately terminated. The CFST performed the entire investigation in only 3 days; 11 days fewer than expected. The result was significant timesaving and reduced investigative fees. In addition, the company had sufficient evidence to protect itself from a wrongful termination suit. The porn operation was shut down and the corporate bandwidth returned to normal, and the company prevented a huge possible liability.

Hands-on Projects

The firm had an instance of an inappropriate email circulating through their network and violating their corporate policy. The firm didn't know where that email originated from, but they were able to interrogate a number of different machines using a CFS. First, the firm was able to identify the source of the email, which was sent externally. Second, they put together an extremely accurate timeline as to what had happened. The reports that the firm was able to generate from the corporate relationship standpoint were excellent. The firm sent information to the director of human relations or the chief operating officer (COO). When the evidence was sent to them, the quality and completeness were such that they rarely asked for more information. The CFS investigation reports were extremely thorough—more than enough information to allow human relations to decide how to move forward with the incident.

Case Project

The challenge in doing further analysis was that the manager in question was located in California, while the investigators were in New Jersey. The CFS was able to do a remote forensic investigation of the manager's computer without drawing suspicion that an investigation was taking place. Upon further analysis, it was determined that the dialog in question was in an email from the manager's spouse, accusing him of vile and unlawful behavior. The couple was going through a bitter divorce proceeding and the accusations were completely unfounded. The investigation was completed in 30 minutes, without the CFS having to travel cross-country, without harming the employee's reputation, and without having to alert anyone outside of corporate security about the potential situation. The organization was able to quickly investigate this potential incident remotely, discreetly, immediately, and cost effectively.

Optional Team Case Project

Within six hours of the CFS's initial involvement with this case, the CFS was able to identify information necessary to support the client's claims. The goal of the investigation was to prove that the files the opposition was using as the basis for the client's product line were indeed a derivative of client's files. The investigation revealed that the files used by the opposition in their manufacturing process possessed the identical metadata of the files originally created by the client. By extracting this vital information, the CFS was able to prove that the files being used by the opposition were taken from the client's computer and modified to suit the opposition's desires. The similarities in document format, font selection, file creation dates, and document metadata would prove to be the compelling evidence the client needed to present their case.

PART V: ADVANCED COMPUTER FORENSICS SYSTEMS AND FUTURE DIRECTIONS

Chapter 20: Advanced Computer Forensics

Review Questions and Exercises

True/False

1. False
2. True

3. False
4. False
5. False

Multiple Choice

1. D
2. B
3. C
4. D
5. E

Exercise

On a case-by-case basis, human resources notifies the company's CFST of reported allegations. The CFST then further investigates and analyzes employee actions including inappropriate material, email abuse, instant messaging, and other nonbusiness-related activity. The CFST is also used to capture evidence, document findings, and produce reports with supporting evidence for submission to all relevant parties. This information assists in proving or disproving the allegations against employees. The CFST enables the employee investigation process to be discreet and thorough, minimizing the potential of creating employee ill-will during investigations and enabling verifiable support of allegations.

Hands-on Projects

This organization was able to investigate machines that may have been compromised by a malicious entity. Instead of pulling machines off the network for analysis and potentially losing valuable information relevant to the investigation, they used a CFST to remotely capture and analyze relevant artifacts critical to the incident. IDS alerts notified the CFST about the suspect machines. The CFST used a snapshot capability to quickly identify unauthorized running processes, who was communicating with the suspect machines, and users currently logged on. This information assisted them in identifying the exact application tunneling through the corporate firewalls and making calls to the Internet. The snapshot information enabled the CFST to thoroughly document the incident and to take appropriate actions for initial remediation. During incident post-analysis, the CFST reviewed findings and implemented new controls to prevent similar incidents from occurring in the future.

Case Project

By proactively acquiring and preserving employees' computer hard drives, they protect themselves from employees denying knowledge or possession of proprietary or confidential data when the employee was notified of termination. In the event of a wrongful termination lawsuit or when defending against employee accusations, the company has a forensic copy of the hard drive. It can be used to prove the employee had knowledge of a particular matter or was in fact exhibiting a particular behavior that was grounds for termination.

Optional Team Case Project

The company uses a CFS to examine employee hard drives and check for claim IDs related to cases that have been determined or suspected as fraudulent. The CFS can match these claim IDs on employee computers and then locate artifacts that may prove employee collaboration. The CFS can also conduct further analysis to locate relevant manipulated and deleted documents on employee computers that can be used to prove or disprove culpability. When incriminating artifacts are identified, the evidence is captured and preserved, which enables the CFS to present the case that an employee was or was not defrauding the company by creating claims for events that didn't actually occur. The entire investigation is performed covertly without creating employee ill-will and without the need for in-person investigations.

Chapter 21: Summary, Conclusions and Recommendations

Review Questions and Exercises

True/False

1. False
2. True
3. False

4. True
5. True

Multiple Choice

1. E
2. C
3. D
4. E
5. A

Exercise

To commence the investigation, the CFST faced difficult barriers. Flying a CFST overseas is impractical because it could require several weeks to coordinate and clear special computer equipment through customs. In addition, on-site business and investigative operations would be compromised. Fortunately, the CFST was able to remotely investigate any computer system in a forensically sound and noninvasive manner anywhere on a wide area network—without disrupting system operations. Prior to using the CFST as standard practice for organizational investigations, employee computer examinations conducted by the company were cumbersome and highly disruptive. Suspect employees would often be alerted to an investigation because of the inability to conduct rapid and discrete investigations. It was not uncommon for machines to "mysteriously" disappear or be destroyed before CFSTs arrived on-site for removal. The use of a CFST introduced a new level of efficiency and efficacy to organization-wide investigative processes, saving the company time and money while dramatically reducing legal and financial exposure.

In addition, the CFST remotely previewed and acquired information from several computers housed in the Middle East office. Upon analysis, they found important evidence pointing toward certain fraudulent actions tied to key individuals. By launching the investigation from the United States, the company saved time and money while validating the financial audit team's suspicion to the point of identifying potential suspects. Coincidentally, this successful analysis took place just before the financial audit team was traveling to the Middle East office to conduct what once was a previously scheduled, routine audit. Armed with hard data, auditors targeted certain individuals with specific questions while at the foreign office. Interview information was then passed on to the U.S. CFST, who used the answers to continue searching for additional evidence. This multidepartmental team approach led to the identification of the employees who eventually admitted to fraudulent activity. Those individuals were swiftly terminated. This case demonstrates how a CFST has enabled timely remote capture of evidence. It allowed investigative teams to identify that fraud had occurred, pinpoint potential suspects and narrow the investigative scope to specific topics and individuals. Overall, the CFST saved this organization time and money, while greatly improving its fraud investigation procedures.

This page intentionally left blank

F Checklists by Chapter

PART I: OVERVIEW OF COMPUTER FORENSICS TECHNOLOGY

Chapter 1: Computer Forensics Fundamentals

Table F1.1 Evidence Identification and Retrieval Checklist Form

Evidence Identification and Retrieval Checklist Form

Date: ________________

The computer forensics specialist should ensure that the following provisional list of actions for retrieval and identification of evidence are adhered to (check all tasks completed):

____ 1. Protect the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.

____ 2. Discover all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.

____ 3. Recover all (or as much as possible of) discovered deleted files.

____ 4. Reveal (to the greatest extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.

____ 5. Access (if possible and legally appropriate) the contents of protected or encrypted files.

____ 6. Analyze all possibly relevant data found in special (and typically inaccessible) areas of a disk. This includes but is not limited to what is called unallocated space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as slack space in a file (the remnant area at the end of a file in the last assigned disk cluster that is unused by current file data, but once again, may be a possible site for previously created and relevant evidence).

____ 7. Print out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data.

____ 8. Provide an opinion of the system layout; the file structures discovered; any discovered data and authorship information; any attempts to hide, delete, protect, and encrypt information; and anything else that has been discovered and appears to be relevant to the overall computer system examination.

____ 9. Provide expert consultation and/or testimony, as required [1].

Table F1.2 Principal Computer Forensic Activities Checklist Form

Principal Computer Forensic Activities Checklist Form

Date: ______________________

The computer forensic specialist should ensure that the following provisional list of actions for some of the principal computer forensic methods are adhered to (check all tasks completed):

____ 1. Safely seize computer systems and files to avoid contamination and/or interference.

____ 2. Safely collect data and software.

____ 3. Safe and noncontaminating copying of disks and other data media.

____ 4. Review and report on data media.

____ 5. Source and review backup and archived files.

____ 6. Recover/reconstruct deleted files—logical methods.

____ 7. Recover material from swap and cache files.

____ 8. Recover deleted/damaged files—physical methods.

____ 9. Core-dump: Collect an image of the contents of the active memory of a computer at a particular time.

____ 10. Estimate if files have been used to generate forged output.

____ 11. Review single computers for proper working during relevant period, including service logs, fault records, and the like.

____ 12. Prove/test reports produced by complex client/server applications.

____ 13. Review complex computer systems and networks for proper working during relevant period, including service logs, fault records, and the like.

____ 14. Review system/program documentation for design methods, testing, audit, revisions, and operations management.

____ 15. Review applications programs for proper working during relevant period, including service logs, fault records, and the like.

____ 16. Identify and examine audit trails.

____ 17. Identify and review monitoring logs.

____ 18. Conduct telecoms call path tracing (PTTs or path-tracing telecoms and telecoms utilities companies only).

____ 19. Review access control services—quality and resilience of facilities (hardware and software, identification/authentication services).

____ 20. Review and assess access control services—quality of security management.

____ 21. Review and assess encryption methods—resilience and implementation.

____ 22. Set up proactive monitoring to detect unauthorized or suspect activity within application programs and operating systems and across local area and wide area networks.

____ 23. Monitor email.

____ 24. Use special alarm or trace programs.

____ 25. Use honeypots.

____ 26. Interact with third parties (suppliers, emergency response teams, and law enforcement agencies).

____ 27. Review and assess measuring devices and other sources of real evidence, including service logs, fault records, and the like.

____ 28. Use routine search programs to examine the contents of a file.

____ 29. Use purpose-written search programs to examine the contents of a file.

____ 30. Reconcile multisource files.

____ 31. Examine telecoms devices and location of associated activity logs and other records perhaps held by third parties.

____ 32. Reconstruct events.

____ 33. Reconstruct complex computer intrusion.

____ 34. Reconstruct complex fraud.

_____ 35. Reconstruct system failure.

_____ 36. Reconstruct disaster affecting computer-driven machinery or process.

_____ 37. Review expert- or rule-based systems.

_____ 38. Reverse compilation of suspect code.

_____ 39. Use computer programs that purport to provide simulations or animations of events: review of accuracy, reliability, and quality.

Chapter 2: Types of Computer Forensics Technology

Table F2.1 Forensics Technology Types Checklist Form

Forensic Technology Types Checklist Form

Date: ____________________

The CFS should ensure that the following provisional list of actions for some of the forensic technology types are adhered to (check all tasks completed):

_____ 1. Move documentary evidence quickly from the printed or typewritten page to computer data stored on floppy diskettes, Zip disks, CDs, and computer hard disk drives.

_____ 2. Create a new type of virtual evidence for e-commerce transactions and email communications over the Internet.

_____ 3. Share computer files over the Internet, when tied to the commission of a crime, (creates a new and novel twist to the rules of evidence and legal jurisdiction).

_____ 4. Keep the venue in mind when criminal activities involve the use of the Internet (venue can be in different cities, counties, states, and/or countries). The evidence needed to prove such computer-related crimes potentially resides on one or more computer hard disk drives in various geographic locations.

_____ 5. Keep in mind that the computer hard disk drives may also be the property of criminals as well as innocent third parties (Internet service providers). Such evidence is commonly referred to as computer evidence, but it is not limited to cases involving computer crimes.

_____ 6. Rely on computer evidence that is connected to a computer crime (not to traditional crimes that are committed using one or more computers as tools in the commission of a crime). Computer crimes are specifically defined by federal and/or state statutes.

_____ 7. Make sure computer evidence resides on computer storage media as bytes of data in the form of computer files and ambient data.

____ 8. Make sure ambient data (which is usually beyond the awareness of most computer users) provides the computer forensics investigator with the element of surprise when computer users are interviewed. For example, a computer user who believes that he or she destroyed the computer evidence may confess when confronted with part or all of the evidence extracted from ambient data sources.

____ 9. Make sure your computer investigations rely on evidence that is stored as data and that the timeline of dates and times of files that were created, modified, and/or last accessed by the computer user are recorded. Timelines of activity can be especially helpful when multiple computers and individuals are involved in the commission of a crime.

____ 10. Make sure your computer forensics investigator always considers timelines of computer usage in all computer-related investigations. The same is true in computer security reviews concerning potential access to sensitive and/or trade secret information stored in the form of computer files. Computer investigations play an important role in cases involving the theft of company trade secrets.

____ 11. Make sure your intellectual property lawyers rely on computer evidence and computer investigations in such cases as stock frauds, financial frauds, and embezzlements. The same is true concerning criminal litigation involving stock frauds, financial frauds, and embezzlements. Much of the evidence related to these types of crimes will be in computer data form. In the past, documentary evidence used to prove these crimes was exclusively in paper form. However, many computer-related communications and transactions are now conducted without paper documents ever being created. Financial fraud investigators have been forced to change the way they do business.

____ 12. Make sure your computer-related investigations involve the review of Internet log files to determine Internet account abuses in businesses or government agencies.

____ 13. Make sure your computer investigations involve the analysis of the Windows swap file.

____ 14. Make sure you use computer forensics procedures, processes, and tools, so that the computer forensics specialist can identify passwords, network logons, Internet activity, and fragments of email messages that were dumped from computer memory during past Windows work sessions. When such leads are identified, they can be perfected through the use of computer forensics text search programs.

____ 15. Use other computer forensics software tools to document the computer evidence once it has been preserved, identified, and extracted.

Chapter 3: Types of Computer Forensics Systems

Table F3.1 Forensics Systems Types Checklist Form

Forensic Systems Types Checklist Form

Date: ____________________

The CFS should ensure that the following provisional list of actions for some of the forensic systems types are adhered to (check all tasks completed):

____ 1. Have procedures in place to establish your organization's security.

____ 2. Have procedures in place to develop your security policy.

____ 3. Have procedures in place to secure the Web client.

____ 4. Have procedures in place to deter masqueraders and ensure authenticity.

____ 5. Have procedures in place to prevent eavesdropping to protect your privacy.

____ 6. Have procedures in place to thwart counterfeiters and forgery to retain integrity.

____ 7. Have procedures in place to avoid disruption of service to maintain availability.

____ 8. Have procedures in place to configure your operating system and network security.

____ 9. Have procedures in place to enhance your Web server security.

____ 10. Have procedures in place to issue and manage certificates.

____ 11. Have procedures in place to examine the impact of security policies.

____ 12. Have procedures in place to identify hacking techniques.

____ 13. Have procedures in place to be able to recognize attacks.

____ 14. Have procedures in place to deploy an IDS.

____ 15. Have procedures in place to commission your IDS.

____ 16. Have procedures in place to manage your IDS.

____ 17. Have procedures in place to install and configure your firewall.

____ 18. Have procedures in place to support outgoing services through firewall configuration.

____ 19. Have procedures in place to secure external services provision.

____ 20. Have procedures in place to protect internal IP services.

____ 21. Have procedures in place to manage your firewall.

____ 22. Have procedures in place to measure risk to avoid disaster.

____ 23. Have procedures in place to design SAN security solutions.

____ 24. Have procedures in place to be able to manage and document the recovery.

____ 25. Have procedures in place to create the recovery plan.

____ 26. Have procedures in place to assure the plan and apply document management.

____ 27. Have procedures in place to analyze and design PKIs.

____ 28. Have procedures in place to implement PKI.

____ 29. Have procedures in place to manage PKI.

____ 30. Have procedures in place to design wireless network security.

____ 31. Have procedures in place to be able to plan for wireless network security.

____ 32. Have procedures in place to install and deploy wireless network security.

____ 33. Have procedures in place to maintain wireless network security.

____ 34. Have procedures in place to be able to implement satellite encryption.

____ 35. Have procedures in place to prevent misuse of satellite encryption technology.

____ 36. Have procedures in place to conduct a privacy-needs audit.

____ 37. Have procedures in place to develop an enterprise privacy plan.

____ 38. Have procedures in place to implement an enterprise privacy plan.

____ 39. Have procedures in place to manage privacy on the enterprise Web site.

____ 40. Have procedures in place to manage privacy on the Internet supply chains.

____ 41. Have procedures in place to design and plan for ID management.

____ 42. Have procedures in place to install and deploy ID management.

____ 43. Have procedures in place to maintain ID management.

____ 44. Have procedures in place to plan for identity theft protection techniques.

____ 45. Have procedures in place to install and deploy identity theft protection techniques.

____ 46. Have procedures in place to deploy enterprise biometrics solutions.

____ 47. Have procedures in place to organize homeland security efforts.

____ 48. Have procedures in place to launch a national cybersecurity awareness and training program.

Chapter 4: Vendor and Computer Forensics Services

Table F4.1 Vendor and Forensics Services Types Checklist Form

Vendor and Forensic Services Types Checklist Form

Date: ____________________

The CFS should ensure that the following provisional list of actions for some of the vendor and forensic services types are adhered to (check all tasks completed):

____ 1. Make sure your computer forensics service provides an analysis of computers and data in criminal investigations.

____ 2. Make sure your computer forensics service provides an on-site seizure of computer data in criminal investigations.

____ 3. Make sure your computer forensics service provides an analysis of computers and data in civil litigation.

____ 4. Make sure your computer forensics service provides an on-site seizure of computer data in civil litigation.

____ 5. Make sure your computer forensics service provides an analysis of the company computers to determine employee activity.

____ 6. Make sure your computer forensics service provides assistance in preparing electronic discovery requests.

____ 7. Make sure your computer forensics service provides reporting in a comprehensive and readily understandable manner.

____ 8. Make sure your computer forensics service provides court-recognized computer expert witness testimony.

____ 9. Make sure your computer forensics service conducts computer forensics on both PC and MAC platforms.

____ 10. Make sure your computer forensics service provides a fast turnaround time.

____ 11. Have procedures in place to employ the latest tools and techniques to recover your data.

____ 12. Have procedures in place to allow you to find your files and restore them for your use.

____ 13. Have procedures in place to allow you to recover even the smallest remaining fragments.

____ 14. Have procedures in place to safeguard your data with such methods as encryption and backup.

____ 15. Have procedures in place to thoroughly clean sensitive data from any computer system you plan on disposing of.

____ 16. Have procedures in place to survey your business and provide guidance for improving the security of your information. This includes such possible information leaks as cordless telephones, cellular telephones, trash, employees, and answering machines.

____ 17. Be cognizant of the IP address limitations for determining the possible attribution of the event you are investigating. Although this process will educate the administrator on how to characterize the threat to his or her company from analyzing IP addresses that appear in the logs, a complete determination of the threat your organization faces is a more involved process.

____ 18. Have procedures in place to investigate the possibility of staffing a professional competitive intelligence cell in your company or sponsoring an assessment of the threat to your company's systems from a group of intelligence and information security specialists.

____ 19. Have procedures in place to know what the threat against your system is as well as its vulnerabilities.

PART II: COMPUTER FORENSICS EVIDENCE AND CAPTURE

Chapter 5: Data Recovery

Table F5.1 Data Recovery Checklist Form

Data Recovery Checklist Form

Date: ____________________

The CFS should ensure that the following provisional list of actions for data recovery are adhered to (check all tasks completed):

____ 1. Make sure you are ready and have procedures in place for disasters like floods, tornadoes, earthquakes, and terrorism when they strike.

____ 2. Make sure you are ready and have a plan in place to take periodic image copies and send them off-site.

____ 3. Perform change accumulation to reduce the number of logs required as input to the recovery, which saves time at the recovery site. However, performing this step consumes resources at the home site.

____ 4. Evaluate your environment to decide how to handle the change accumulation question/problem in action/task #3.

____ 5. Have procedures in place to implement your plan.

____ 6. Check your assets to make sure they're ready as part of your plan.

____ 7. Build your recovery JCL correctly. JCL is tricky, and you need to get it exactly right. Data integrity and your business rely on this task.

____ 8. Clean your RECON data sets. It can take hours if done manually, and it's an error-prone process. When your system is down, can you afford to make mistakes with this key resource?

____ 9. Test your plan. There's a lot to think about. In the real world, there's much more.

____ 10. Make sure your plan works before you are required to use it.

____ 11. Have procedures in place to deal with issues of increased availability, shrinking expertise, growing complexity, failures of many types, and the costs of data management and downtime.

Chapter 6: Evidence Collection and Data Seizure

Table F6.1 Evidence Collection and Data Seizure Checklist Form

Evidence Collection and Data Seizure Checklist Form

Date: ____________________

The CFS should ensure that the following provisional list of actions for evidence collection and data seizure are adhered to (check all tasks completed):

____ 1. Make sure that once you've created a master copy of the original data, you don't touch it or the original itself—always handle secondary copies.

____ 2. Have procedures in place to document the nature, extent, and reasons for changes to the data.

____ 3. Make sure you understand what you are doing, because you have to be able to account for any changes you made and describe exactly what you did. If you ever find yourself out of your depth, either learn more before continuing (if time is available) or find someone who knows the territory.

____ 4. Make sure your plan of action is not based on trial and error. No one is going to believe you if they can't replicate your actions and reach the same results.

____ 5. Work fast, so that there is a less likelihood that the data is going to change.

____ 6. Always try to collect the most volatile evidence first, because some electronic evidence is more volatile than others. You should proceed from volatile to persistent evidence.

____ 7. Never, ever shut down a system before you collect the evidence.

____ 8. Avoid rebooting at all costs. It is even worse than shutting a system down and should be avoided. As a general rule, until the compromised disk is finished with and restored, it should never be used as a boot disk.

____ 9. Any programs you use should be on read-only media (such as a CD-ROM or a write-protected floppy disk) and should be statically linked. Because the attacker may have left trojaned (trojan horse) programs and libraries on the system, you may inadvertently trigger something that could change or destroy the evidence you're looking for.

____ 10. Make sure your planning stage takes place prior to any investigator arriving at the computer crime scene, including two ways to structure a team of investigators.

____ 11. Make sure that you have good case management software. It can go a long way in easing the burden of carrying out a search and seizure.

Chapter 7: Duplication and Preservation of Digital Evidence

Table F7.1 Duplication and Preservation of Digital Evidence Checklist Form

Duplication and Preservation of Digital Evidence Checklist Form

Date: ________________

The computer forensics specialist should ensure the following are adhered to (check all tasks completed):

____ 1. Shut down the computer.

____ 2. Document the hardware configuration of the system.

____ 3. Transport the computer system to a secure location.

____ 4. Make bit-stream backups of hard disks and floppy disks.

____ 5. Mathematically authenticate data on all storage devices.

____ 6. Document the system date and time.

____ 7. Make a list of key search words.

____ 8. Evaluate the Windows swap file.

____ 9. Evaluate file slack.

____ 10. Evaluate unallocated space (erased files).

____ 11. Search files, file slack, and unallocated space for keywords.

____ 12. Document file names, dates, and times.

____ 13. Identify file, program, and storage anomalies.

____ 14. Evaluate program functionality.

____ 15. Document your findings.

____ 16. Retain copies of software used.

____ 17. Establish a solid relationship with local law enforcement, as they will be a valuable resource in the evidence collection process [1].

Chapter 8: Computer Image Verification and Authentication

Table F8.1 Computer Image Verification and Authentication Checklist Form

Computer Image Verification and Authentication Checklist Form

Date: ____________________

The computer forensics specialist should ensure the following are adhered to (check all tasks completed):

____ 1. Alter the data on the cartridge. To successfully subvert the *digital integrity verification and authentication* protocol, it would be necessary to do the following without detection: either in a manner that ensures that the relevant data block produces the same hash value or that the relevant hash value is recalculated and inserted into the vault, (1) recalculate all the subsequent derivative hash values; (2) recalculate and rewrite the relevant encrypted block; break the seals on the relevant *digital integrity verification and authentication* floppy disks; and rewrite the data and repair the seals.

____ 2. Alter the data on the machine and then re-DIBS® it (if the machine in question was available). This would require the original DIBS drive; the original password known only to the copying officer (and encrypted on each cartridge in the series); exact knowledge of the date and time settings within the computer at the time of the original copy; and either a similarly numbered tamperproof bag on which the defendant's signature would be forged, or the original bag opened and resealed with the new floppy inside.

____ 3. Examine and analyze any discrepancies between the defendant's floppy disk and that of the investigators to determine whether such discrepancies disqualified any or all of the copied data. The digital integrity of the floppy disk and the physical integrity of the tamperproof bag are, in this case, the arbiters of whether such discrepancies were deliberately manufactured.

____ 4. Make sure the digital integrity of any element in the chain (cartridges and floppies) is verified independently of the others (especially through the inclusion of the encryption phase). It is, thus, useless for a defendant to destroy his or her floppy disk in the hope that its absence will assist any challenge to the *digital integrity verification and authentication* protocol.

____ 5. Make sure that security-conscious CIOs meet with their counterparts to discuss security issues with their senior executives, have a dedicated chief security officer, perform a formal assessment of security risk, conduct simulated security breaches, force users to change passwords more frequently, and consult with vendors about their own security precautions.

____ 6. Take steps to make sure security is a higher priority for your company.

PART III: COMPUTER FORENSICS ANALYSIS

Chapter 9: Discovery of Electronic Evidence

Table F9.1 Discovery of Electronic Evidence Checklist Form

Discovery of Electronic Evidence Checklist Form

Date: ________________

The computer forensics specialist should ensure the following are adhered to (check all tasks completed):

____ 1. Do not alter discovered information.

____ 2. Always back up discovered information.

____ 3. Document all investigative activities.

____ 4. Accumulate the computer hardware and storage media necessary for the search circumstances.

____ 5. Prepare the electronic means needed to document the search.

____ 6. Ensure that specialists are aware of the overall forms of information evidence that are expected to be encountered as well as the proper handling of this information.

____ 7. Evaluate the current legal ramifications of information discovery searches.

____ 8. Back up the information discovery file or files.

____ 9. Start the lab evidence log.

____ 10. Mathematically authenticate the information discovery file or files.

____ 11. Proceed with the forensic examination.

____ 12. Find the MD5 message digest for the original information discovery file or files.

____ 13. Log all message digest values in the lab evidence log.

____ 14. When forensic work is complete, regenerate the message digest values using the backups on which work was performed; log these new values alongside the hashes that were originally generated. If the new values match the originals, it's reasonable to conclude that no evidence tampering took place during the forensic examination of the information file(s).

____ 15. Briefly compare the physical search and seizure with its logical (data-oriented) counterpart, information discovery.

Chapter 10: Identification of Data

Table F10.1 Identification of Data Checklist Form

Identification of Data Checklist Form

Date: ________________

The computer forensics specialist should ensure the following are adhered to (check all tasks completed):

____ 1. Use NTP for security reasons.

____ 2. Buy special radios that interpret the signals and send them out on serial (and even parallel) cables to the computers that will serve as your top stratum. WWV broadcasts time signals over short wave, so this information is available worldwide.

____ 3. Use GPS devices. GPS relies on accurate timekeeping for calculating position and movement. GPS devices are fairly inexpensive, although you'll want to buy ones that already have drivers written for them.

____ 4. Remember to have multiple sources. Note that most Cisco Systems routers and switches come with NTP software and are ready for use as NTP servers. (You should disable this service if you're not using it.)

____ 5. Keeping all your systems synchronized to accurate time is not a luxury. Good timekeeping is important to many security functions, such as electronic transactions, certain authentication systems, and, in particular, any forensics activity that might ever be required of you. If you find yourself comparing logs from disparate systems, you'll be exceedingly grateful that you decided to implement NTP.

Chapter 11: Reconstructing Past Events

Table F11.1 Reconstructing Past Events Checklist Form

Reconstructing Past Events Checklist Form

Date: ________________

The computer forensics specialist should ensure the following are adhered to (check all tasks completed):

____ 1. Create a timeline to reconstruct the events that led to your system being corrupted. This can be particularly difficult when it comes to computers—clock drift, delayed reporting, and differing time zones can create confusion in abundance.

____ 2. Do not change the clock on an affected system.

____ 3. Record any clock drift and the time zone in use, as you will need this later, but changing the clock just adds in an extra level of complexity that is best avoided.

____ 4. Synchronize the log files. Log files usually use timestamps to indicate when an entry was added, and these must be synchronized to make sense.

____ 5. Use timestamps. You're not just reconstructing events; you are making a chain of events that must be accounted for as well.

____ 6. Use the GMT time zone when creating your timestamps, because the incident may involve other time zones than your own. Using a common reference point can make things much easier.

____ 7. Make sure you have a dedicated host for the job when analyzing backups. This examination host should be secure, clean (a fresh, hardened install of the operating system is a good idea), and isolated from any network—you don't want it tampered with while you work, and you don't want to accidentally send something nasty down the line.

____ 8. Commence analysis of the backups once the system is available. Making mistakes at this point shouldn't be a problem—you can simply restore the backups again if required.

____ 9. Document everything you do. Remember the mantra.

____ 10. Ensure that what you do is not only repeatable, but that you always get the same results.

____ 11. Reconstruct the chain of events leading to and following the attacker's break-in now that you have collected the data.

____ 12. Make sure you correlate all the evidence you have gathered (which is why accurate timestamps are critical). It's probably best to use graphical tools, diagrams, and spreadsheets.

____ 13. Include all of the evidence you've found when reconstructing the attack—no matter how small it is, you may miss something if you leave a piece of evidence out.

____ 14. Review audit trails of system activity to pinpoint how, when, and why the incident occurred, since the amount of damage that occurred with an incident can be assessed.

Chapter 12: Networks

Table F12.1 Networks Checklist Form

Networks Checklist Form

Date: ____________________

The computer forensics specialist should ensure the following are adhered to (check all tasks completed):

____ 1. Provide expert data visualization techniques to the problem of network data pattern analysis.

____ 2. Apply standard research and analysis techniques to datasets provided by a company or organization.

____ 3. Apply the lessons learned from company-provided datasets to open datasets as the research advances.

____ 4. Provide initial datasets, project initiation, and training in network traffic datasets and analysis techniques.

____ 5. Provide expert network forensic rule-based algorithms for incorporation by researchers.

____ 6. Repeatedly test and verify new visualization techniques and procedures to ensure that new patterns are, in fact, accurate representations of designated activities.

____ 7. Develop a test database.

____ 8. Develop a design methodology for visualizing test data.

____ 9. Develop a query interface to the database.

____ 10. Map data structures to a visualization model.

____ 11. Build a prototype.

____ 12. Refine a prototype.

____ 13. Incorporate live Internet data.

____ 14. Test live Internet data.

____ 15. Deliver a final build.

____ 16. Produce new visualization techniques to streamline and enhance analysis of network forensic data.

____ 17. Produce a Web browser–compatible prototype that demonstrates these techniques to visualize and query vast amounts of data. The resulting interactive visualization interface will advance the usability of the system, solve the volumetric problem with analyzing these datasets, and advance the adaptation of the solution in the INFOSEC market.

____ 18. Routinely archive all email as it is received on your server for a certain period of time (for example, 30–60 days).

____ 19. Clear the archives after an additional specified time.

____ 20. Physically segregate the backup copies of the email system from backups of the rest of the computer system.

____ 21. Automatically erase email from the computer system, including backups, after a short period (15–30 days).

____ 22. Apply uniform retention and deletion standards and features outside the server to workstations and laptops.

____ 23. Formulate and distribute a statement that the automatic deletion of electronic records will be suspended and steps taken to preserve records in the event of investigation or litigation.

____ 24. Maintain an appropriate SOP document. All agencies that seize and/or examine digital evidence must do this.

____ 25. Clearly set forth in this SOP document all elements of an agency's policies and procedures concerning digital evidence, which must be issued under the agency's management authority.

____ 26. Review the SOPs on an annual basis to ensure their continued suitability and effectiveness.

____ 27. Make sure the procedures you use are generally accepted in the field or supported by data gathered and recorded in a scientific manner.

____ 28. Maintain written copies of appropriate technical procedures.

____ 29. Use hardware and software that is appropriate and effective for the seizure or examination procedure.

____ 30. Record all activity relating to the seizure, storage, examination, or transfer of digital evidence in writing.

____ 31. Make sure all digital evidence is available for review and testimony.

____ 32. Make sure that any action that has the potential to alter, damage, or destroy any aspect of original evidence is performed by qualified persons in a forensically sound manner.

____ 33. Be alert. One of the best ways to ensure that your network is secure is to keep abreast of developing threats. Security experts agree that ignorance is the most detrimental security problem. Most hacks occur because someone wasn't paying attention. Web sites such as the CERT home page (*http://www.cert.org*) are excellent places to get current information.

____ 34. Apply all service patches. Many companies will sit on patches rather than put them to use. Others are not diligent enough about searching for and downloading the latest virus definitions. Smart hackers bank on the negligence of others.

____ 35. Limit port access. Although just about any application that uses TCP requires a port, you can minimize exposure by limiting the number of ports accessible through a firewall. NNTP (Network News Transport Protocol) is an excellent example: unless your shop requires newsgroup access, port 119 should be shut down.

____ 36. Eliminate unused user IDs and change existing passwords. Poor maintenance is almost as dangerous as ignorance.

____ 37. Make sure system administrators routinely audit and delete any idle user IDs.

____ 38. Make sure that in order to limit the likelihood of successful random guessing, all user and system passwords be system-generated or system-enforced.

____ 39. Avoid the use of simple network management protocol (SNMP) across the firewall.

____ 40. Check routers to make sure they do not respond to SNMP commands originating outside the network.

____ 41. Secure remote access. Try to break into your own network. You can learn a lot by hacking into your own system.

____ 42. Test your packet-filtering scheme. If you can gain access to your systems from a workstation outside your network, you can easily test your packet-filtering scheme without any outside exposure. If you do spot a weakness, you'll be one step ahead of the hackers.

____ 43. Ask a consultant when in doubt. If you don't have the technical wherewithal in-house or if your staff is too busy working on other projects, don't hesitate to call in a consultant. Many companies offer security assessment and training services.

____ 44. Assess your company's networking needs and shut down any ports that aren't necessary for day-to-day operations, such as port 53 for DNS access and port 119 for NNTP services.

____ 45. Be sure to eliminate unused user IDs and to avoid provisioning SNMP services through the firewall.

PART IV: COUNTERMEASURES: INFORMATION WARFARE

Chapter 13: Fighting Against Macro Threats: Defensive Strategies for Governments and Industry Groups

Table F13.1 Defensive Strategies for Governments and Industry Groups Checklist Form

Defensive Strategies for Governments and Industry Groups Checklist Form

Date: ________________

The CFS should ensure that the following provisional list of actions for preparing for defensive strategies for governments and industry groups are adhered to (check all tasks completed):

____ 1. Implement leadership. Who should be in charge in the government? An immediate and badly needed first step is the assignment of a focal point for federal government leadership in support of a coordinated U.S. response to the strategic IW threat. This focal point should be located in the Executive Office of the President, because only at this level can the necessary interagency coordination of the large number of government organizations involved in such matters—and the necessary interactions with the Congress—be effectively carried out.

____ 2. Establish leadership responsibility with industry. The Executive Office should also have the responsibility for close coordination with industry, because the nation's information infrastructure is being developed almost exclusively by the commercial sector. Once established, this high-level leadership should immediately take responsibility for initiating and managing a comprehensive review of national-level strategic IW issues.

____ 3. Conduct an immediate risk assessment. The federal government leadership entity should, as a first step, conduct an immediate risk assessment to determine, to the degree possible, the extent of the vulnerability of key elements of current U.S. national security and national military strategy to strategic information warfare.

____ 4. List the components of this review. Strategic target sets, IW effects, and parallel vulnerability and threat assessments should be among the components of this review. In an environment of dynamic change in both cyberspace threats and vulnerabilities, there is no sound basis for presidential decision making on strategic IW matters without such a risk assessment.

____ 5. Create a robust national information infrastructure. In this context, there is always the hope or the belief that the kind of aggressive response can be delayed while cyberspace gets a chance to evolve robust defenses on its own. This is, in fact, a possibility—that the healing and annealing of an immune system that is under constant assault, as cyberspace is and assuredly will continue to be, will create the robust national information infrastructure that everyone hopes to use. But it may not, and we're certainly not there now.

____ 6. Address the government's role. The appropriate role for government in responding to the strategic IW threat needs to be addressed, recognizing that this role (certain to be part leadership and part partnership with the domestic sector) will unquestionably evolve.

____ 7. Facilitate and maintain information systems and the infrastructure. In addition to being the performer of certain basic preparedness functions (such as organizing, equipping, training, and sustaining military forces), the government may play a more productive and efficient role as facilitator and maintainer of some information systems and infrastructure; through policy mechanisms such as tax breaks to encourage reducing vulnerability and improving recovery and reconstitution capability.

____ 8. Establish a new traditional change in the government's role. An important factor is the traditional change in the government's role as one moves from national defense through public safety toward things that represent the public good. Clearly, the government's perceived role in this area will have to be balanced against public perceptions of the loss of civil liberties and the commercial sector's concern about unwarranted limits on its practices and markets.

____ 9. Establish a national security strategy. Once an initial risk assessment has been completed, U.S. national security strategy needs to address preparedness for the threat as identified. Preparedness will cross several traditional boundaries from "military" to "civilian," from "foreign" to "domestic," and from "national" to "local."

____ 10. Create a minimum essential information infrastructure (MEII) as a possible strategic defensive IW initiative. The MEII is conceived as that minimum mixture of U.S. information systems, procedures, laws, and tax incentives necessary to ensure that the nation continues functioning even in the face of a sophisticated strategic IW attack.

____ 11. Maintain the strategic nuclear Minimum Essential Emergency Communications Network (MEECN). One facet of such an MEII might be a set of rules and regulations sponsored by the federal government to encourage the owners and operators of the various national infrastructures to take measures to reduce their infrastructure's vulnerability or to ensure rapid reconstitution in the face of IW-type attacks.

____ 12. At an early date conduct an assessment of the feasibility of an MEII. The MEII construct is conceptually very attractive even though there was some uncertainty as to how it might be achieved.

____ 13. Establish a national military strategy. The current national military strategy emphasizes maintaining U.S. capability to project power into theaters of operation in key regions of Europe and Asia. Because of the emerging theaters of operation in cyberspace for such contingencies, strategic IW profoundly reduces the significance of distance with respect to the deployment and use of weapons. Therefore, battlefield command, control, communications, and intelligence (C3I) vulnerabilities may become less significant than vulnerabilities in the national infrastructure.

____ 14. Create a plan for a national military strategy. Planning assumptions fundamental to current national military strategy are obsolescent. Consideration of these IW features should be accounted for in U.S. national military strategy.

____ 15. Make sure the U.S. military plan and strategy is not vulnerable to IW attack. Against this difficult projection and assessment situation, there is the ever-present risk that the United States could find itself in a crisis in the near term, facing the possibility of, or indications of, a strategic IW attack. When the president asks whether the United States is under IW attack (and, if so, by whom) and whether the U.S. military plan and strategy is vulnerable, a foot-shuffling "we don't know" will not be an acceptable answer.

____ 16. Implement the new IW strategy. It must be acknowledged that strategic IW is a very new concept that is presenting a wholly new set of problems. These problems may well yield to solution—but not without the intelligent and informed expenditure of energy, leadership, money, and other scarce resources.

Chapter 14: The Information Warfare Arsenal and Tactics of the Military

Table F14.1 Information Warfare Arsenal and Tactics of the Military Checklist Form

Information Warfare Arsenal and Tactics of the Military Checklist Form

Date: ________________

The CFS should ensure that the following provisional list of actions for preparing for information warfare arsenal and tactics of the military are adhered to (check all tasks completed):

____ 1. Review of the military organization's mission. The first suggested action involves a review of the military organization's mission in light of the emerging threat. A few military organizations may find that IW-D adds a mission or increases the importance of an existing mission.

____ 2. Review new relationships. New relationships with external organizations may be required, or perhaps existing relationships may need to be modified. Thus, a review of these relationships is in order.

____ 3. Allocate responsibilities. Who is responsible for IW-D in the military organization? Perhaps the military organization has a chief information officer (CIO) and it would be appropriate for the CIO to take on this responsibility. Perhaps the responsibility for IW-D is spread out among several individuals. In any event, a clear allocation of responsibilities is required.

____ 4. Identify which information and systems are critical. Not all information or all systems should be considered equal with respect to the protection they merit. It is important, given resource constraints, to identify which information and systems (and functions of these systems) are critical and which are not critical.

____ 5. Conduct a vulnerability analysis. How vulnerable are the information and systems? What is the specific nature of the vulnerabilities? Answers are needed to provide a basis for planning and developing defenses. It needs to be remembered that vulnerabilities are relative to the threat, the nature of which is constantly evolving. Thus, vulnerability analyses are not a one-time task but must be part of a continuing effort.

____ 6. Develop a comprehensive IW-D strategy. Isolated actions to improve security are helpful, but they are not a substitute for the development of a comprehensive IW-D strategy for a military organization.

____ 7. Develop a plan to manage risks. Because it is not possible to avoid all the risks associated with IW, each military organization needs to develop a plan to manage these risks.

____ 8. Discuss the issues. In the course of developing and articulating a military organizational IW-D strategy and risk-management plan, many issues will be raised and discussed. These discussions will create a greater awareness of the problem within the military organization and improve the organization's ability to meet the challenges associated with IW-D.

____ 9. Review investment strategies and supporting technologies. Combating IW is a long-term proposition. There are many long poles in the tent. A military organization's investment strategies need to be reviewed, and investments in defenses and supporting technologies must be made.

____ 10. Reallocate resources. Some reallocation of resources may be made necessary by changes in the operating costs associated with introducing new procedures and safeguards.

Chapter 15: The Information Warfare Arsenal and Tactics of Terrorists and Rogues

Table F15.1 Information Warfare Arsenal and Tactics of Terrorists and Rogues Checklist Form

Information Warfare Arsenal and Tactics of Terrorists and Rogues Checklist Form

Date: ________________

The CFS should ensure that the following provisional list of actions for preparing for information warfare arsenal and tactics of terrorists and rogues are adhered to (check all tasks completed):

____ 1. Default settings for software products sold to consumers should be at the highest level of security.

____ 2. Nations developing information strategies should consider investment, both intellectually and financially, across the gamut of information operations.

____ 3. Air power's pervasiveness and speed are advantages in the face of transnational and transregional terror. In an era when terrorism may take place across the globe and sponsors may cross national and regional lines, the global sight and reach of Air Force assets should be valuable to national decision makers.

____ 4. Air and space power should not always be the instruments of choice in the U.S. counterterrorism arsenal. They can, however, play an important role in intelligence and covert action.

____ 5. Air and space power should rarely be used independently; instead, they will have a synergistic effect with other counterterrorism instruments such as covert action, diplomacy, economic instruments, and joint military operations. The same instruments may be used in parallel against terrorist supporters, terrorist infrastructure and networks, and terrorists themselves.

____ 6. Air power in the service of counterterrorism should include, but also go beyond, surveillance and punishment of state sponsors.

____ 7. Deterrence and response should probably evolve in the direction of a more "personalized" approach emphasizing the monitoring and attack of key nodes in terrorist networks and the forcible apprehension of individual terrorist suspects.

____ 8. Demands on air power should be driven as much by the requirement to intercept and extract suspects as by the need to attack training camps or strike supporting regimes.

____ 9. Air and space power should help make terrorism—an increasingly amorphous phenomenon—more transparent.

____ 10. The ability to identify and target terrorist-related activity and help expose terrorism and its sponsors for policy action and international censure should be key contributions of Air Force assets.

____ 11. As terrorism becomes more diffuse and its sponsorship increasingly hazy, finding the "smoking gun" should become more difficult but essential to building a consensus for action.

____ 12. Space-based sensors, surveillance by unmanned air vehicles, and signals intelligence should facilitate the application of air power and other counterterrorist capabilities.

____ 13. Counterterrorism should increasingly focus on urban areas and thus face strong operational constraints. For political reasons, terrorists find key targets in cities. The use of air power for counterterror, therefore, faces the more general problem of operating in urban environments, a situation where the difficult Israeli experience in Beirut and south Lebanon is instructive.

____ 14. The value of air power here should depend on its capacity for discriminate targeting and less-than-lethal technologies.

Chapter 16: The Information Warfare Arsenal and Tactics of Private Companies

Table F16.1 Information Warfare Arsenal and Tactics of Private Companies Checklist Form

Information Warfare Arsenal and Tactics of Private Companies Checklist Form

Date: ________________

The CFS should ensure that the following provisional list of actions for preparing for information warfare arsenal and tactics of private companies are adhered to (check all tasks completed):

____ 1. It is recommended that, traditionally, private companies be organized in a hierarchical way and also be viewed as such. Much like a Norman *mote and bailey* castle, where a keep on a central raised mound was encircled by a ditch and a picket, private companies are viewed as entities that are, or should be, impervious to the outside world, allowing entry only at designated, protected points. Once within the structure, movement up to the pinnacle of command is meant to be within certain set parameters, and deviation from these parameters is not encouraged.

____ 2. Flat management structures, it is recommended, should make the internal passage within the corporate entity somewhat less linear. Flat management does not allow for free ingress from the outside as one of its goals—it may allow for more points of contact between points inside the structure and outside, but these are monitored and controlled.

____ 3. Over the years, layers of protection have accreted around the structure, much like the walls that were thrown up around the keeps of concentric castles. All of these concentric defenses should repeat the pattern of controlled and protected points of ingress and egress.

____ 4. The growth of the information network and the increasing porosity of corporate entities should lead to a rethinking of the reliance on concentricity and control of entrances.

____ 5. Corporate entities should have new points of ingress (such as telephony and Internet access points)—consumers demand it. Added to this intentional accumulation of entry points must be those that are either unwittingly left open by a corporate entity, because the advances of technology are not understood, or those that are left open through intention or negligence, where the possibility of unwanted or uncontrolled ingress is appreciated, but nothing is done about it.

____ 6. Attention should also be paid to points of egress. Much damage can be done by an information outflow caused by a disgruntled employee.

____ 7. A hierarchical corporation, based on a fortress structure, may be vulnerable if an information flow is disrupted. This may be so even where a flat management structure exists within the fortress. The entity may be hard put to regroup and function without great delay.

____ 8. A corporate entity based on a network may be much better placed to respond to a potentially disabling attack. Diversified information and command lines should be called into action and utilized should one line be cut. Such a corporation would be able to continue its core operations in a much shorter timeframe than a defensive-fortress structure. This does not mean to say that a corporation should abandon all controls of ingress and egress, and open its doors to the world. Defenses from cyberterrorism should be put in place. This discussion highlights the first primary step in risk management—identification.

____ 9. Potential threats should be identified and provided for. A simple treatment of defensive structures may not be wise, because the chaotic nature of the information network and the development of new technologies will inevitably mean that new forms of attacks and new holes in the armor will always open, often in unexpected places.

____ 10. A diversified command-and-control structure, and the duplication of information supplies should go some way in both treating current risk and coping with problems when unforeseen or currently nonexistent risks appear.

Chapter 17: The Information Warfare Arsenal of the Future

Table F17.1 Preparation for the Information Warfare Arsenal of the Future Checklist Form

Information Warfare Arsenal of the Future Checklist Form

Date: ________________

The computer forensics specialist should ensure the following actions are adhered to (check all tasks completed):

____ 1. Identify substate groups who have embraced the information revolution, as has the rest of society. Going a stage further and attacking the NII can certainly be an attractive option for substate groups. However, as the Provisional Irish Republican Army (PIRA) case shows, to inflict even a portion of the disruption that the doomsday mongers suggest would require a tremendous investment in intelligence preparation of the battlefield (IPB), not to mention actually implementing the assault. More technology-savvy groups such as environmental protesters may be the first to use offensive IW techniques but they will have limited aims and not pose a national security threat. It is likely to be some time yet before professional cyberterrorists become a significant IW threat.

____ 2. Institute a review of national vulnerabilities to an IW arsenal of the future. This prospect leaves governments with a window of opportunity that needs to be seized. In the past, states have tended to react to changing terrorist threats rather than preempting them, and the substate group usually retains the initiative. This may also be the case with cyberterrorism. As yet, though, there has not been national leadership of the sort provided by the White House and the Congress.

____ 3. Proactively monitor the threat. Performing a holistic assessment of national vulnerabilities and creating a rigorously enforced information assurance program can meet this new threat. Although it is obvious that the American NII is far more vulnerable to the IW arsenal of the future than the British NII, because of the far higher level of connectivity, there is little room for complacency. For once, the British government, in conjunction with its European partners, has the opportunity of staying ahead of an emerging threat from terrorist and other substate groups. It will not be long before substate groups graduate from exploiting the Internet for propaganda to using it offensively.

____ 4. Conduct strategic IW campaigns. The introduction of nonnuclear electromagnetic bombs into the IW arsenal of a modern air force considerably broadens the options for conducting strategic campaigns. Clearly, such weapons are potent force multipliers in conducting a conventional war, particularly when applied to electronic combat, offensive counterair (OCA), and strategic air attack operations.

____ 5. Develop the use of IW weapons responsibly. The massed use of such IW weapons would provide a decisive advantage to any nation with the capability to effectively target and deliver them. The qualitative advantage in capability so gained would provide a significant advantage even against a much stronger opponent not in the possession of this capability.

____ 6. Commit to strategic IW campaigns. Electromagnetic weapons, however, open up less conventional alternatives for the conduct of a strategic campaign, which derive from their ability to inflict significant material damage without inflicting visible collateral damage and loss of life. Western governments have been traditionally reluctant to commit to strategic campaigns, as the expectation of a lengthy and costly battle, with mass media coverage of its highly visible results, will quickly produce domestic political pressure to cease the conflict.

____ 7. Develop a strategy of graduated response. In this strategy, an opponent who threatens escalation to a full-scale war is preemptively attacked with electromagnetic weapons to gain command of the electromagnetic spectrum and command of the air. Selective attacks with electromagnetic weapons may then be applied against chosen strategic targets to force concession. Should these fail to produce results, more targets may be disabled by electromagnetic attack. Escalation would be sustained and graduated to produce steadily increasing pressure to concede the dispute. Air and sea blockades are complementary means via which pressure may be applied.

____ 8. Develop advanced electromagnetic weapons. Because electromagnetic weapons can cause damage on a large scale very quickly, the rate at which damage can be inflicted can be very rapid, in which respect such a campaign will differ from the conventional, where the rate at which damage is inflicted is limited by the usable sortie rate of strategic air attack capable assets.

____ 9. Implement a full-scale conventional strategic air attack campaign. Should blockade and the total disabling of vital economic assets fail to yield results, these may then be systematically reduced by conventional weapons, to further escalate the pressure. Finally, a full-scale conventional strategic air attack campaign would follow to wholly destroy the hostile nation's war-fighting capability.

____ 10. Use the strategy of graduated response. Other situations where electromagnetic bombs may find useful application is in dealing with governments that actively implement a policy of state-sponsored terrorism or infoterrorism, or alternately choose to conduct a sustained low-intensity land warfare campaign. Again, the strategy of graduated response, using electromagnetic bombs in the initial phases, would place the government under significant pressure to concede.

____ 11. Regulate nanotechnology because of its immense abuse potential.

____ 12. Do not use advanced nanotechnology to build small self-replicating machines that can feed on organic matter—a bit like bacteria but much more versatile, and potentially more destructive than the H-bomb.

Chapter 18: Surveillance Tools for Information Warfare of the Future

Table F18.1 Surveillance Tools for Information Warfare of the Future Checklist Form

Surveillance Tools for Information Warfare of the Future Checklist Form

Date: ________________

The computer forensics specialist should ensure the following actions are adhered to (check all tasks completed):

____ 1. Use electromagnetic devices. As a punitive weapon, electromagnetic devices are attractive for dealing with belligerent governments. Substantial economic, military, and political damage may be inflicted with a modest commitment of resources by their users, and without politically damaging loss of life.

____ 2. Use cookies wisely and visitors will appreciate their value. Use them gratuitously and visitors will resent the intrusion. It's up you to help keep cookies from being the most unpalatable junk food on the Web.

____ 3. Get rid of the ability to link to Web images from Word documents. There really is no solution to being able to track Word documents using Web bugs. Because this linking ability is a useful feature, the Privacy Foundation does not recommend its removal.

____ 4. Do not disable Web browser cookies inside of Word documents.

____ 5. Use a program such as ZoneAlarm (*http://www.zonelabs.com/store/content/home.jsp*) to warn about Web bugs in Word documents. ZoneAlarm monitors all software and warns if an unauthorized program is attempting to access the Internet. ZoneAlarm is designed to catch trojan horses and spyware. However, because Word typically does not access the Internet, ZoneAlarm can also be used to catch bugged Word documents.

____ 6. The data to be mined should have a direct connection to the goal task, and the new information should be directly applicable to the task situation.

____ 7. Collect appropriate data. Think first about what kind of information is needed and how it will be used.

____ 8. If the data already exist, understand its strengths and limitations as they relate to the task specification and the available data-mining techniques.

____ 9. Consider alternative data sources.

____ 10. Augment the existing data with additional data.

____ 11. Alter the objectives if no additional data can be obtained and the existing data is inadequate for the original task specification.

Chapter 19: Civilian Casualties: The Victims and Refugees of Information Warfare

Table F19.1 Civilian Casualties: The Victims and Refugees of Information Warfare Checklist Form

Civilian Casualties: The Victims and Refugees of Information Warfare Checklist Form

Date: ________________

The computer forensics specialist should ensure the following actions are adhered to (check all tasks completed):

____ 1. Make sure that general or centralized monitoring of communications are not a chief or central component of the government's response to computer security.

____ 2. Give other activities (notably the identification and closing of existing vulnerabilities) higher priority.

____ 3. Reject the authority for increased monitoring of information systems.

____ 4. Strengthen the underlying laws for monitoring communications systems and accessing stored data.

____ 5. Limit the role of the FBI and the NSA in computer security: it has been demonstrated that their surveillance agendas trump their protective missions, and their activities are often so cloaked in secrecy as to generate understandable suspicion.

____ 6. Oversight of infrastructure protection should be institutionalized within the executive branch and should be accessible to the public.

____ 7. There should be established within the executive branch appropriate mechanisms for oversight of computer security issues, involving both industry representatives and privacy advocates.

____ 8. Congress must follow this issue carefully and should insist on periodic reports on the status, scope, and effectiveness of critical infrastructure activities, with special focus on monitoring and intrusion detection initiatives and the protection of privacy.

____ 9. Limit the government's role in private sector infrastructure protection, even though the cyber masses acknowledge the need for government participation, especially in educating society about what is at stake.

____ 10. The private sector should set information security standards, and the government should clearly define and limit what information it seeks from businesses and how that information will be used.

PART V: ADVANCED COMPUTER FORENSICS SYSTEMS AND FUTURE DIRECTIONS

Chapter 20: Advanced Computer Forensics

Table F20.1 Advanced Computer Forensics Checklist Form

Advanced Computer Forensics Checklist Form

Date: ________________

The computer forensics specialist should ensure the following actions are adhered to (check all tasks completed):

____ 1. Install patches.

____ 2. Secure old computers: inventory your systems, and unplug from the network any that no one uses anymore.

____ 3. If a networked computer is shared, make sure it receives the same security updates as other systems.

____ 4. Encrypt data every place it's stored, including PC hard drives.

____ 5. Perform frequent security audits, including trying to gain access using easily available hacking tools.

____ 6. Ensure that you only run the services you need and only open the ports needed by your network.

____ 7. Make sure your gateway to the Internet is a system without any important company data or a hardware solution backed up by a firewall.

____ 8. Always check security bulletins and consider joining hacking mailing groups to find out what's happening on the other side of computer security.

____ 9. Regularly test the security yourself; then you know what to find solutions for.

____ 10. Make sure no one person controls the system front to back.

____ 11. Require every person logging-on to use a password.

____ 12. Assign supervisory rights to as few people as possible.

____ 13. Back up all systems weekly.

____ 14. Have a strict sign-in/sign-out system for backup tapes.

____ 15. Always have a current copy of the backup tape stored remotely.

____ 16. Perform backups of desktops and laptops as well as servers.

____ 17. Rotate backup tapes—don't use the same one over and over again.

____ 18. Change passwords every three months.

____ 19. Keep servers in a secured area.

____ 20. Stay up-to-date on software patches.

____ 21. Use intrusion detection software that alerts you when you are being hit.

____ 22. Make sure two pairs of eyes have checked code before it is entered into the system.

____ 23. Have an information security department (at least one person and then one other for every 1,000 users) that is separate from the IT department and reports directly to the chief information officer.

____ 24. Spend at least 6 to 8% of the IT budget on information security.

____ 25. Train information security personnel to be aware of any employee who shows signs of being troubled or disgruntled, particularly if that employee holds an information-critical position.

____ 26. Beef up security during certain events, such as mergers or downsizings, that could upset workers and cause them to lash out at the company.

____ 27. Monitor the network—set up software that will alert you if someone is working in a different part of the network or at a different time than usual.

____ 28. Scan email to see what's going out of the company; double-check backup tapes and have someone else do the backups if that person is the one in question.

____ 29. Make sure the person in charge of the system is not the same person in charge of the backup.

____ 30. Have specific policies and punishments built into employee contracts.

____ 31. Make sure critical IT workers are bonded.

____ 32. Change everyone's passwords so he or she can't use them to break into the system.

____ 33. Verify that your backup tapes are where they should be; make sure the information has been saved correctly and the tape is functioning properly.

____ 34. Do a new backup.

____ 35. Lock down every system that a terminated employee had access to on the day of termination.

____ 36. Have a new network administrator ready to step into the open position immediately.

____ 37. Go up on the system and check user names and passwords, looking for anything unusual.

____ 38. Make sure there's a password for every logon.

____ 39. Lock down all the inside doors, such as the file servers, application servers, and mail servers.

____ 40. Look for back doors on the system.

____ 41. Make sure there aren't any known vulnerabilities that haven't been patched—the administrator could have left those holes behind so he could get back in.

____ 42. Strengthen your intrusion detection system.

____ 43. Set a trip wire—software that alerts the administrator to system anomalies, such as the size of a file changing.

REFERENCES

[1] Robbins, Judd, "An Explanation of Computer Forensics," National Forensics Center, 774 Mays Blvd. #10-143, Incline Village, NV 89451, 2004 [The Computer Forensics Expert Witness Network, 472 Scenic Drive, Ashland, OR 97520, 2004]. (© 2004, National Forensics Center. All rights reserved), 2001.

This page intentionally left blank

G About the CD-ROM

CD-ROM FOLDERS

Products: A collection of forensic tools, demonstrations, and docs.
Figures: All of the figures from the book, in folders by chapter. There are no folders for chapters with no figures.

SYSTEM REQUIREMENTS

Please visit the developer Web sites listed in this appendix for exact system requirements, FAQs, updates, ordering information, licenses, and links to other tools and sources. Nevertheless, the minimum system requirements for all of these software products include Adobe Acrobat 5.0 or higher, Windows 2000, XP, and 2003 and WinZip, as well as an Internet connection; some also require basic hardware such as: Firewire, USB devices, Zip, Jaz, floppy diskettes, or hard disk drives (IDE, EIDE, SCSI, ATA, SATA).

PRODUCTS

The following forensic tools, demos, documentation, and presentations are included on the accompanying CD-ROM.

The information contained on the CD-ROM is the property of the respective developers. It may not be distributed without their permission. Inquiries regarding the software contained on the CD-ROM should be directed to the developers of the products. In addition, please review the publisher's disclaimer at the beginning of the book. The developers in this appendix and CD-ROM are listed in alphabetical order, followed by a list of software products and documentation. When accessing the CD-ROM for a particular developer, just click on the developer's name (folder), and a list of software products and documentation files/folders will be displayed for you to access.

Also, a number of the companies' contributions include large numbers of support files which are not meant to be opened directly by the user (for example, LC Technology, ManTech Security & Mission Assurance and New Technologies, Inc.). For these, it is indicated in the list of companies below which files the users should be able to access directly. The filename and/or the entire folder (if all the files can be opened by the user) have been added after the product name, and all other files in that folder are support files and not meant to be opened by the user.

Finally, please read all of the text files (.txt) that accompany each developer file and folder. Inside most of the text files are the files needed to create the program disks and manuals. Just read and follow the instructions carefully before accessing any .exe file.

ACR Data Recovery, Inc.

4487 Park Drive, Suite B Norcross, GA 30093 USA

Products:

Media Tools Professional, Media Tools Manual

Phone: 800-444-3225; 770-925-4420

Fax: 770-925-8808

http://www.atl-datarecovery.com

ACR provides a full-scale data recovery center, computer forensic software (Media Tools Professional and Media Tools Manual), and in-house services to corporations and individuals. They also offer software for do-it-yourself recovery situations.

Computer Forensics Inc.

1749 Dexter Avenue North, Seattle, Washington 98109

Products (documents/presentations):

Discovery of Databases in Litigation, Instant Messenger Programs, Ten Steps to Successful Computer Discovery, Ten Ways to Torpedo Your Data Discovery Expert

Phone: 206-324-6232

Fax: 206-322-7318

email: cfinc@forensics.com

http://www.forensics.com/

Computer Forensics Inc. offers services in electronic discovery, forensic analysis, expert witness services, and risk control programs for companies.

Computer Forensics Labs

14 Inverness Drive East B-140, Englewood, CO 80112
Products (documents/presentations):
File Structure Taxonomy, Forensic Examination Checklist
Phone: 800-625-6451; 303-649-1181
Fax: 303-649-1697
http://www.computerforensiclabsinc.com/

CFL specializes in the use of advanced forensic, analytical, and recovery techniques for reconstruction and preservation of data.

CyberEvidence

5 Grogan's Park, Suite 211, The Woodlands, TX 77380
Products (documents/presentations):
Articles, Online training manuals and presentations, Newsletters
Phone: 281-296-0465
http: //www.cyberevidence.com

CyberEvidence, Inc., is a computer forensics company that provides both training and services. The computer forensics training classes run all year and are available for both the novice and the advanced investigator. The computer forensic investigations service helps companies and law firms conduct forensic data recovery for policy violations or litigation support.

CY4OR

Northern office:
CY4OR Limited, 116a Bury New Road, Whitefield, Manchester, M45 6AD
Phone: 0161-767-8123
Fax: 0161-766-2225
Southern Office:
CY4OR Limited, 7 Midshires Business Park, Smeaton Close, Aylesbury, Bucks, HP19 8HL

Products (documents/presentations):
Are You Sitting Next to a Criminal?
Phone: 01296-488123
Fax: 01296-488124
http://www.cy4or.co.uk/

CY4OR is a computer forensics company that provides proactive and reactive computer forensic investigation services to the public and private sector including law enforcement agencies, solicitors, and corporate companies.

Digital Mountain, Inc.

1762 Technology Drive, Suite 204, San Jose, CA 95110
Products (documents/presentations):
Where Data Resides—Data Discovery from the Inside Out
Phone: 866-DIG-DOCS (866-344-3627)
Fax: 408-327-0544
info@digitalmountain.com; *http://www.digitalmountain.com*

Digital Mountain is a provider of computer forensics, electronic discovery, network forensics, and electronic management services on a national basis. They also provide expert witness services for law firms and enterprises.

e-fense, Inc.

Corporate Headquarters:
120 N. Saint Asaph St., Alexandria, VA 22314
Products (documents/presentations):
Helix and GRAB
Phone: 800-793-8205
http://www.e-fense.com/

e-fense, Inc. is a certified computer forensic professionals firm that offers computer forensics, network security, and electronic discovery. They have offices in Colorado, Texas, Virginia, and Washington, DC.

eMag Solutions

3495 Piedmont Road, Eleven Piedmont Center, Suite 500,
Atlanta, GA 30305

Products (documents/presentations):

Data recovery, Electronic discovery, Exchange server data recovery, Facts about tape, MMPC, MMTMS, Novell GroupWise data recovery, Optical conversion recovery

Phone: 800-364-9838; 404-995-6060

Fax: 800-334-8273; 404-872-8247

http://www.emaglink.com/

Based in the U.S. and U.K., eMag provides computer forensic software and services.

Forensicon, Inc.

53 W. Jackson Boulevard, Suite 603, Chicago, IL 60604

Products (documents/presentations):

Electronic Evidence Best Practices

Phone: 312-427-5667

Fax: 312-427-5668

http://www.forensicon.com/

Forensicon, Inc., provides top-notch assistance to law firms and corporations nationwide in expert computer forensics and electronic discovery services.

Guidance Software Inc

215 North Marengo Ave., Second Floor, Pasadena, CA 91101

Products (documents/presentations):

Career Track Program, Corporate, eDiscovery Services, EnCase Enterprise, EnCase Forensic, EnCase Snapshot, EnCase Legal Journal, EnCE Certification, FastBloc, litigation support, professional services, PSD-IR Program, training option programs and training

Phone: 626-229-9191

Fax: 626-229-9199

http://www.guidancesoftware.com/

Guidance Software's Professional Services Division offers expertise in computer forensics and enterprise investigations. As the creator of EnCase®, the most widely used computer forensics tool, Guidance Software combined its staff of seasoned law enforcement and corporate investigators to create a team of consultants offering technical services, forensics labs, and a direct link to legal and engineering support.

Kroll Ontrack Inc.

9023 Columbine Road, Eden Prairie, MN 55347

Products (documents/presentations):

Computer Forensics Case Profiles, "Computer Forensics Process Graphic," "Where Can You Find Email? Graphic"

Phone: 800-347-6105 (7:30 A.M. – 5:30 P.M. CST, weekdays)

http://www.krollontrack.com

Kroll Ontrack provides a wide range of services, consulting, and software to help locate, review, and retrieve electronic evidence.

LC Technology International Inc.

28100 US Hwy 19 N., Suite 203, Clearwater, FL 33761

Products (software):

LC Technology's Forensic Utility Suite: FPRO-DEMO Folder (recovery_demo.exe Help\English\index.html, FPROlicense.txt), FRWIN-DEMO (recovery_demo.exe,help\English\index.html, FRW-license.txt), PR3-DEMO (PRGUIDemo.exe, PRLanguage.exe,PR-license.txt), autorun.exe.

Phone:

Sales: 866-603-2195
Customer Service: 727-449-0891
Technical Support: 727-449-0891
Fax: 727-449-0893

Email:

Sales: Sales @ LC-Tech.com
Support: Support @ LC-Tech.com
Customer Service: Service @ LC-Tech.com
Training: Training @ LC-Tech.com
Investigations: Investigations @ LC-Tech.com
Press: Press @ LC-Tech.com

Europe:

High Pavement Business Centre, 3-5 High Pavement, Nottingham,
UK NG1 1HF

Phone: +44 (0)115 9596490

Fax: +44 (0)115 989 7301

Email: kenc@lc-tech.com

http://www.lc-tech.co.uk

Asian Distributor:

American Megatrends Inc., Japan, 6-13-11, Mikuni BLDG.8F, Sotokanda,
Chiyoda-ku, Tokyo 101-0021, Japan

Phone: +81-3-5812-0020

http://www.amij.com

LC Technology manufactures undelete and recovery software and offers computer forensic training classes in its Florida training facility.

ManTech Security & Mission Assurance

12015 Lee Jackson Hwy, Fairfax, VA 22033

Products (software):

NwReader/Setup.exe

Phone: 703-218-6000; 703-218-8200

http://www.mantech-ist.com

ManTech Security & Mission Assurance specializes in providing secure, environment-tailored computer forensics, information assurance, and information system security support to federal, state, and local intelligence, defense, law enforcement, and corporate customers.

New Technologies, Inc.

2075 Northeast Division Street, Gresham, Oregon 97030 USA

Products (software):

Read First—NTA Stealth Demo Instructions; NTA Stealth Demo (NTA.exe, NTA 60.pdf, ntasflop.pdf, ntasusb.pdf, and ntavqsi.pdf) and a copy of the NTA Viewer program (NTAVIEW.exe and NTAVIEW.pdf)

Phone: 503-661-6912

Email: info@forensics-intl.com

Forensics Web site: *http://www.forensics-intl.com*
Security Web site: *http://www.secure-data.com*
Litigation support Web site: *http://www.dataforensics.com*

New Technologies, Inc. works primarily with large companies and government agencies in the field of forensic consultation, training, and risk assessment.

Project Leadership Associates

250 S. Wacker Dr., Suite 345, Chicago, IL 60606
Products (documents/presentations):
CALSM article and Electronic Data Discover Sheet
Phone: 312-441-0077
Fax: 312-441-0088
http://www.projectleadership.net

Project Leadership Associates offers expertise in computer forensics, data analysis, and expert testimony.

Renew Data

9500 Arboretum Blvd., Suite L2-120, Austin, TX 78759
Products (documents/presentations):
RenewData Electronic Evidence Services Brochure
Phone: 512-276-5500 (office); 888-811-3789
Fax: 512-276-5555
http://www.renewdata.com

Renew Data supplies the legal community with services including consulting, retrieving, and restoring data, analyzing forensic results, and expert witness testimony.

Total Recall (BinaryBiz North America)

700 Ken Pratt Blvd., Suite 204-171, Longmont, CO 80501
Products (software):
VirtualLab and iDriveRepair (please note the file vLabAuth in vLabAuth.zip is a support file and you are not meant to run it directly.)
Phone: 800-743-0594
http://www.binarybiz.com

Total Recall (BinaryBiz North America) offers computer forensics and both in-lab data recovery as well as advanced remote data recovery to companies and individuals around the world. They count over 80,000 successful recoveries.

Vogon International Data Recovery

Talisman Business Centre, Talisman Road, Bicester OX26 6HR, UK

Products (software):

> Digital fingerprints containing MD5, SHA-1 and SHA-512; newsletters; Forensic Software 4pp; Imaging System 4pp; Lab Forensic Works; Mobile Forensic Works; and VICAR 6

Phone: +44 (0) 1869 355255

Fax: +44 (0) 1869 355256

http://www.vogon-international.com

Based in the U.K., Germany, and the U.S., Vogon rescues data from all types of disks, tape media, storage devices, files, databases, and email and operating systems. They also have a forensic and investigative department for all sorts of forensic services and training. They are capable of detecting, analyzing, and presenting computer evidence in the broadest range of criminal activities. Reports produced by their investigation service comply with legal requirements for admissibility in court, and they can provide expert witnesses to give evidence.

H Glossary of Terms and Acronyms

2600
A hacker organization whose main product is *2600* magazine. This publication has (at times) been considered the premier hacker print product.

8lgm
Eight (8) Little Green Men hacker group that compiles and distributes security tips.

Abuse of privilege
Formal nomenclature for user action not in accordance with organizational policy or law. Actions falling outside, or explicitly proscribed by, acceptable use policy.

Acceptable level of risk
A judicious and carefully considered assessment by the appropriate authority that a computing activity or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of assets, threats and vulnerabilities, countermeasures, and operational requirements.

Acceptable use policy (AUP)
DoD nomenclature for documented standards or guidance on usage of information systems and networked assets.

Accountability
The principle that individuals using a facility or a computer system must be identifiable. With accountability, violations or attempted violations of system security can be traced to individuals who can then be held responsible.

Accuracy
DoD parlance for the notion that information has been maintained and transferred in such a way as to be inviolate (the information has been protected from being modified or otherwise corrupted either maliciously or accidentally). Accuracy protects against forgery or tampering. Typically invoked as a synonym for integrity.

Acme of skill
To subdue an adversary without killing him.

Active attack
A form of attack in which data is actually modified, corrupted, or destroyed.

Adapter
A device that serves as an interface between the system unit and a device attached to it, such as a SCSI Adapter. Often synonymous with expansion card or board. Can also refer to a special type of connector.

Advanced WWW Counter

Full-featured advanced counter that is highly customizable, allowing you to change digit formats, colors, time, and adjustable data counts.

Ambient data

This is a forensic term that describes, in general terms, data stored in nontraditional computer storage areas and formats. The term was coined in 1996 to help students understand computer-evidence-processing techniques that deal with evidence not stored in standard computer files, formats, and storage areas. The term is now widely used in the computer forensics community and it generally describes data stored in the Windows swap file, unallocated space, and file slack.

Anomaly detection

A label for the class of intrusion detection tactics that seek to identify potential intrusion attempts by virtue of their being (presumably) sufficiently deviant (anomalous) in comparison with expected or authorized activities. Phrased another way, anomaly detection begins with a positive model of expected system operations and flags potential intrusions on the basis of their deviation (as particular events or actions) from this presumed norm.

Anonymous FTP

Allows visitors to upload or download predetermined files from designated directories without usernames or passwords. For example, distribute your latest software package by allowing visitors to download it through an anonymous ftp. This is different from a regular ftp account

Antivirus

Software that detects, repairs, cleans, or removes virus-infected files from a computer.

Application

A more technical term for program.

Application gateway

One form of a firewall in which valid application-level data must be checked or confirmed before allowing a connection. In the case of an ftp connection, the application gateway appears as an ftp server to the client and an ftp client to the server.

ASIM
(automated security incident measurement)

Current DoD automated security tool that monitors network traffic, collects information on targeted unit networks, and detects unauthorized network activity.

Assurance

A measure of confidence that the security features and architecture of an information system or network accurately reflect and enforce the given security policy.

Asynchronous attacks

Attacks that take advantage of dynamic system actions—especially by exploiting an ability to manipulate the timing of those actions.

Attack

With specific regard to IW—a specific formulation or execution of a plan to carry out a threat. An attempt to bypass security controls on a computer. An active attack alters data. A passive attack releases data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Attitudes

Positively or negatively learned orientations toward something or someone that have a tendency to motivate an individual or group toward some behavior. Experienced soldiers, for example, have negative attitudes toward slovenliness.

Audit trail

In computer security systems, a chronological record of when users login, how long they are engaged in various activities, what they were doing, and whether any actual or attempted security violations occurred. An automated or manual set of chronological records of system activities that may enable the reconstruction and examination of a sequence of events or changes in an event.

AUP

Acronym for acceptable use policy.

Autoresponders

Sends an automated email response to incoming mail sent to a specific address. For instance, you can have your visitors send an email to info@yourdomain.com to get an email explaining your latest product or automatically reply to orders with a prewritten thank you email message.

Back door

A hole in the security of a computer system deliberately left in place by designers or maintainers. Synonymous with trap door. A hidden software or hardware mechanism used to circumvent security controls. A breach created intentionally for the purpose of collecting, altering, or destroying data.

Bandwidth

Bandwidth is the sum of all the data transferred from and to your Web site, including email, Web pages, and images. See "Monthly Traffic."

Bank

The collection of memory chips or modules that make up a block of memory. This can be one, two, or four chips. Memory in a PC must always be added or removed in full-bank increments.

Basic psyop study (BPS)

A detailed background document that describes the psyop-relevant vulnerabilities, characteristics, insights, and opportunities that are known about a specific country susceptible to exploitation.

Battlefield visualization

The process whereby the commander develops a clear understanding of the current state with relation to the enemy and environment, envisions a desired end-state that represents mission accomplishment, and then subsequently visualizes the sequence of activity that moves the commander's force from its current state to the end-state.

Battlespace

The field of military operations circumscribed by the aggregate of all spatial (geographic range, altitude) and virtual (communicational connectivity) dimensions in which those operations are realized. This is a generic term connoting no limitation to the geographical constraints suggested by the term *battlefield*. Components are determined by the maximum capabilities of friendly and enemy forces to acquire and dominate each other on the ground and in the electromagnetic spectrum.

Between-the-lines entry

Access that an unauthorized user gets, typically by tapping the terminal of a legitimate user that is inactive at the time.

BIOS

The part of the operating system that provides the lowest level interface to peripheral devices. The BIOS is stored in the ROM on the computer's motherboard.

BLOB

Binary large object used to describe any random large block of bits, usually a picture or sound file; can be stored in a database but is normally not interpretable by a database program. Can be used as a mild hacker threat (mailbomb) when mailed. Can also be used to hide malicious logic code.

Blue box devices

Gadgets created by crackers and phone hackers ("phreakers") to break into the telephone system and make calls bypassing normal controls and billing procedures.

BMC4I

Battle(space) management command, control, communications, and intelligence. Briefly stated, the overall label for those components and processes comprising the "nervous system" of a modern military force in a theater of operations. The planning, tasking, and control of the execution of missions through an architecture of sensors, communications, automation, and intelligence support.

Boot

To start up your computer. Because the computer gets itself up and going from an inert state, it could be said to lift itself up "by its own bootstraps"—this is where the term *boot* originates.

Boot Record

Once the BIOS determines which disk to boot from, it loads the first sector of that disk into memory and executes it. Besides this loader program, the boot record contains the partition table for that disk. If the boot record is damaged, it can be a very serious situation.

Bootstrap

To load and initialize the operating system on a computer. Often abbreviated to boot.

Bulletin board

Web-based message forum where visitors can read, post, and reply to messages or questions left by other visitors.

Bus

A set of conductors (wires or connectors in an integrated circuit) connecting the various functional units in a computer. There are busses both within the CPU and connecting it to external memory and peripheral devices. The bus width (i.e., the number of parallel connectors) is one factor limiting a computer's performance.

C2

Acronym for command and control.

C2 attack

Sometimes written "C2-attack." Abbreviation for command-and-control attack. Any action against any element of the enemy's command-and-control system.

C2 counterwar

Presumed synonym for command-and-control counterwar.

C2 protect

Abbreviation for command-and-control protect.

C2W

Acronym for command-and-control warfare.

C3

Acronym for command, control, and communications.

C3I

Acronym for command, control, communications, and intelligence.

C4I

Acronym for command, control, communications, computers, and intelligence.

C4ISR

Acronym for command, control, communications, computer intelligence, surveillance, and reconnaissance.

Cache

(Internet browser) The files and graphics saved locally from Web sites you have previously visited.

Card

A circuit board that is usually designed to plug into a connector or slot. See also "Adapter."

Center of gravity

A term commonly encountered that connotes a component or feature of a given system (an adversary's deployed instrumentality) that is critical to either (a) the viability of that given system and/or (b) the viability of the supersystem within which that given system is a participating component.

CERT

Acronym for computer emergency response team. Supports others in enhancing the security of their computing systems; develops standardized set of responses to security problems; provides a central point of contact for information about security incidents; and assists in collecting and disseminating information on issues related to computer security, including information on configuration, management, and bug fixes for systems.

CGI-BIN

CGI stands for common gateway interface. It's simply a way for your visitor's computer to communicate with programs, such as shopping-cart scripts, on your server. The CGI-BIN is a special directory where you store executable programs, such as shopping-cart scripts and counters, on the server. If you don't have access to a CGI-BIN directory, you can't run programs (scripts) on your Web site.

CGI email

Allows you to custom-build email results from a Web page form, much like a mail merge letter.

CIP

Acronym for critical infrastructure protection.

Click

To click an item means to point to it with the screen pointer and then press quickly and release the left mouse button at once.

Cluster

Windows allocates space to files in units called clusters. Each cluster contains from 1 to 64 sectors, depending on the type and size of the disk. A cluster is the smallest unit of disk space that can be allocated for use by files.

CMOS

A part of the motherboard that maintains system variables in static RAM. It also supplies a real-time clock that keeps track of the date, day, and time. CMOS setup is typically accessible by entering a specific sequence of keystrokes during the POST at system start-up.

Cold boot

Starting or restarting a computer by turning on the power supply. See also "Warm boot."

Computer evidence

Computer evidence is quite unique when compared to other forms of documentary evidence. Unlike paper documentation, computer evidence is fragile, and a copy of a document stored in a computer file is identical to the original. The legal "best evidence" rules change when it comes to the processing of computer evidence. Another unique aspect of computer evidence is the potential for unauthorized copies to be made of important computer files without leaving behind a trace that the copy was made. This situation creates problems concerning the investigation of the theft of trade secrets (client lists, research materials, computer-aided design files, formulas, and proprietary software).

Computer forensics

Computer forensics deals with the preservation, identification, extraction, and documentation of computer evidence. The field is relatively new to the private sector but it has been the mainstay of technology-related investigations and intelligence gathering in law enforcement and military agencies since the mid-1980s. Like any other forensic science, computer forensics involves the use of sophisticated technology tools and procedures, which must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer-evidence processing. Typically, computer forensic tools exist in the form of computer software. Computer forensic specialists guarantee accuracy of evidence-processing results through the use of time-tested evidence-processing procedures and through the use of multiple software tools, developed by separate and independent developers. The use of different tools that have been developed independently to validate results is important to avoid inaccuracies introduced by potential software design flaws and software bugs. It is a serious mistake for computer forensics specialists to put "all of their eggs in one basket" by using just one tool to preserve, identify, extract, and validate the computer evidence. Cross-validation through the use of multiple tools and techniques is standard in all forensic sciences. When this procedure is not used, it creates advantages for defense lawyers who may challenge the accuracy of the software tool used and thus the integrity of the results. Validation through the use of multiple software tools, computer specialists, and procedures eliminates the potential for errors and the destruction of evidence.

Computer investigations

Computer investigations rely on evidence stored as data and the timeline of dates and times that files were created, modified, and last accessed by the computer user. Timelines of activity can be especially helpful when multiple computers and individuals are involved in the commission of a crime. The computer forensics investigator should consider timelines of computer usage in all computer-related investigations. The same is true in computer security reviews concerning potential access to sensitive or trade secret information stored in the form of computer files.

Context menu

Also called a "context-sensitive menu," or a "shortcut menu," a context menu includes the commands that are commonly associated with an object on the screen. To activate an item's context menu, point to it with the screen pointer, then press and release the right mouse button once.

Cookies

(Internet browser) Holds information on the times and dates you have visited Web sites. Other information can also be saved to your hard disk in these text files, including information about online purchases, validation information about you for members-only Web sites, and more.

CPU

Stands for central processing unit, a programmable logic device that performs all the instruction, logic, and mathematical processing in a computer.

Crash

A sudden, usually drastic failure. Can be said of the operating system or a particular program when there is a software failure. A disk drive can crash because of hardware failure.

Cross-linked files

Two files that both refer to the same data.

Customizable missing docs page

By placing a file in your main directory called missing.html, you will be able to provide a customized page to any browser that requests a file that does not exist on your server. You can use it to steer visitors to your front page, so you don't lose them if they click on a bad link somewhere.

CyberCash

Used for secure processing of credit-card transactions. It actually takes the payment information and sends it via the banking gateways to obtain real-time approvals for credit cards and checks.

Data

Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. A representation of facts, concepts, or instructions suitable for communication, interpretation, or processing by humans or computers.

Data-driven attack

A form of attack that is encoded in seemingly innocuous data that is executed by a user's or other software to implement an attack. In the case of firewalls, a data-driven attack is a concern because it may get through the firewall in data form and launch an attack against a system behind the firewall.

Datum

Any numerical or geometrical quantity or set of such quantities that may serve as reference or base for other quantities. Where the concept is geometric, the plural form is *datums* in contrast to the normal plural *data*.

DBA

Acronym for dominant battlespace awareness.

DBK

Acronym for dominant battlespace knowledge.

Deception

Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him or her to react in a manner prejudicial to his or her interests.

Decision

In an estimate of the situation, a clear and concise statement of the line of action intended to be followed by the commander as the one most favorable to the successful accomplishment of the mission.

Defense information infrastructure (DII)

A label for the composite information assets of DoD (the American defense establishment).

Defensive counterinformation

Actions protecting the military information functions from the adversary.

Defragment

As modern file systems are used and files are deleted and created, the total free space becomes split into smaller noncontiguous blocks. Eventually new files being created, and old files being extended, cannot be stored each in a single contiguous block but become scattered across the file system. This degrades performance as multiple seek operations are required to access a single fragmented file. Defragmenting consolidates each existing file and the free space into a contiguous group of sectors. Access speed will be improved as a result of reduced seeking. A nearly full disk system will fragment more quickly. A disk should be defragmented before fragmenting reaches 10%.

Degradation of service

Any reduction (with respect to norms or expectations) in a service processes' reaction or response time, quantitative throughput, or quality parameters. This term is often used to denote the general set of service impairments that at the extreme (total degradation to a "zero state" with respect to the given parameters) constitutes an absolute denial of service. Note that (owing to operational constraints such as "time before timing out" settings) a disruptive tactic capable of only degrading service may result in a complete denial of said service from the perspective of the end user.

Denial of service

Actions that prevent any part of an automated information system (AIS) from functioning in accordance with its intended purpose. Denial of service attacks may include denying services or processes limited to one host machine. However, the term is most often invoked to connote action against a single host (or set of hosts), which results in the target's inability to perform services for other users— particularly over a network. One may consider denial of service to be the extreme case of degradation of service in which one or more normal functional parameters (response, throughput) get "zeroed out," at least as far as the end user is concerned. It is important to note that denial is delineated with respect to whether the normal end user(s) can exploit the system or network as expected. Seen in this light, denial (like degradation) is descriptive of a functional outcome and is not therefore definitive with respect to cause (tactics effecting said result). Forms of attack not geared to denial per se may lead to denial as a corollary effect (when a system administrator's actions in response to an intrusion attempt lead to a service outage). As such, denial of service is not a good criterion for categorizing attack tactics.

Denial time

The average length of time that an affected asset is denied to the organization. The temporal extent of operational malaise induced by a denial of service attack.

DII

Acronym for defense information infrastructure.

Direct information warfare

Changing the adversary's information without involving the intervening perceptive and analytical functions.

Directed-energy protective measures

That division of directed-energy warfare involving actions taken to protect friendly equipment, facilities, and personnel to ensure friendly effective uses of the electromagnetic spectrum that are threatened by hostile directed-energy weapons and devices.

Directory

An index into the files on your disk. It acts as a hierarchy and you will see the directory represented in Windows looking like manila folders.

Disk space

The amount of storage space you're allocated to use on the server; also server space and Web space. The more disk space you have, the bigger your Web site can be. It's used to store everything related to your Web site such as your regular html files, images, multimedia files, anonymous ftp files, POP mail messages, CGI scripts, and any other files that make up your Web site.

DMA

Stands for direct access memory. DMA is a fast way of transferring data within a computer. Most devices require a dedicated DMA channel (so the number of DMA channels that are available may limit the number of peripherals that can be installed).

Domain name registration

A domain name is a textual address that is a unique identifier for your Web site and that corresponds to your site's numerical Internet protocol (IP) address and is usually related to your business, such as *www.acmecatapults.com.*

DRAM

Dynamic random access memory (see also "SDRAM"). A type of memory used in a PC for the main memory (such as your 32 Mbytes of RAM). *Dynamic* refers to the memory's memory of storage—basically storing the charge on a capacitor. Specialized types of DRAM (such as EDO memory) have been developed to work with today's faster processors.

Driver

A program designed to interface a particular piece of hardware to an operating system or other software.

Economic info-warfare/economic information warfare

The application of IW tactics to leverage one's interests in the economic realm. A subclassification of IW.

Economic warfare

Aggressive use of economic means to achieve national objectives.

EIDE

Stands for enhanced integrated drive electronics. A specific type of attachment interface specification that allows for high-performance, large-capacity drives. See also "IDE."

Electromagnetic intrusion

The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or causing confusion.

Electronic warfare

Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or attack the enemy. Also called EW.

Electronics intelligence (ELINT)

Technical and geolocation intelligence derived from foreign noncommunications, electromagnetic radiations emanating from sources other than nuclear detonations or radioactive sources.

Electronics security

The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations (radar). This term is also (more loosely) used to connote the topical area or task specialization focusing on achieving this type of protection.

Electro-optical intelligence (ELECTRO-OPTINT)

Intelligence other than signals intelligence derived from the optical monitoring of the electromagnetic spectrum from ultraviolet (0.01 micrometers) through far infrared (1,000 micrometers).

ELINT

Acronym for electronics intelligence.

Email accounts (POP3)

Your email boxes on a server that can be accessed directly to retrieve your mail using such programs as Outlook Express and Netscape Mail. Each POP3 has its own password to ensure privacy, so each of your employees can have their own email address.

Email aliases

Your main POP account for your domain allows the system to capture any name that may be sent to your domain name. This means as long as the @yourdomain.com is proper, any name in front of it will be delivered to your main POP account. Each alias can be forwarded or redirected to any other address of your choice.

Email forwarding

Any email address at your domain may be configured to forward to any other real internet email address. For example, sales@yourname.com can forward to you@aol.com if you like.

Email mini mailing lists

Can be used to send your customers news and updates about your product or services without emailing each one separately. Visitors can add themselves to your list or take themselves off automatically. You send one email and it goes to every email address on the list. The system is capable of multiple lists, each of which can handle up to 1,000 email addresses and outgoing messages up to 75 K each.

Entrapment

The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations.

Essential elements of friendly information

Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness.

Executable

A binary file containing a program in machine language that is ready to be executed (run). Windows machines use the filename extension .exe for these files.

Expansion card

An integrated circuit card that plugs into an expansion slot on a motherboard to provide access to additional peripherals or features not built into the motherboard. See also "Adapter."

Extract

To return a compressed file to its original state. Typically, to view the contents of a compressed file, you must extract it first.

FDISK

The disk-partitioning program used in other operating systems to create the master boot record and allocate partitions for the operating system's use.

File

A collection of data grouped into one unit on a disk.

File allocation table

(FAT or FAT32) The FAT links together all of the clusters belonging to each file, no matter where they are on disk. The FAT is a critical file: you should be sure to back it up regularly. FAT32 is a newer type of FAT, which was designed to handle large hard disks. The older FAT (FAT16) can only support partitions up to two gigabytes in size. FAT32 can handle partitions that are thousands of gigabytes.

File slack

File slack potentially contains randomly selected bytes of data from computer memory. This happens because Windows normally writes in 512-byte blocks called "sectors." Clusters are made up of blocks of sectors. If there is not enough data in the file to fill the last sector in a file, Windows makes up the difference by padding the remaining space with data from the memory buffers of the operating system. This randomly selected data from memory is called "RAM slack" because it comes from the memory of the computer. RAM slack can contain any information that may have been created, viewed, modified, downloaded, or copied during work sessions that have occurred since the computer was last booted. Thus, if the computer has not been shut down for several days, the data stored in file slack can come from work sessions that occurred in the past.

File system

A system for organizing directories and files, generally in terms of how it is implemented in the disk-operating system.

Firewall

A metaphorical label for a set of hardware and software components protecting system resources (servers, LANs) from exogenous attack via a network (from Internet users) by intercepting and checking network traffic. The mix of hardware and software accomplishing firewall operations can vary. For LAN installations of any size, the typical approach is to install one or more computers positioned at critical junctures (gateways) and dedicated to the firewall functions. It is typically the case that such installations are configured such that all external connections (modems, ports) are outside the firewall (with respect to its domain of protection), or at least abut it on its external face. The firewall's own internal connection into the protected domain is typically the focus of monitoring functions. A firewall is also a system or combination of systems that enforces a boundary between two or more networks or a gateway that limits access between networks in accordance with local security policy. The typical firewall is an inexpensive micro-based Unix box kept clean of critical data, with numerous modems and public network ports on it but only one carefully watched connection back to the rest of the cluster.

Firewall machine

A specific computer dedicated to effecting a firewall.

Firmware

Software contained in a read-only memory (ROM) device.

First-wave war(fare)

The term for the mode or character of warfare exemplified in primitive, pastoral, and agricultural societies and dating from prehistory.

Fishbowl

A defensive IW tactic in which a suspicious or unauthorized user is permitted to continue established access to the protected system or network, but whose interactions with that system or network are (unknown and unapparent to the subject) encapsulated within a secure domain of operations (rerouted to an isolated computer or redirected to a dummy environment simulating an actual server) so that IW defenders can observe and analyze the user's intentions, tactics, and identity. To contain, isolate, and monitor an unauthorized user within a system in order to gain information about the user.

Fog of war

The aggregate of factors that reduce or preclude situational certainty in a battlespace.

Fork bomb

A disruptive piece of code directed toward a Unix-based system that causes runaway "forking" (splitting or replication) of operating system processes to degrade or (if saturation is achieved) deny that target system's operations. Code that can be written in one line of code on any Unix system; used to recursively spawn copies of itself, explode, and eventually eat all the process table entries. It effectively locks up the system.

Formmail

Use formmail to email the contents of forms on your Web page to you when a visitor fills it out.

Fragmentation

The state of having a file scattered around a disk in pieces rather than existing in one contiguous area of the disk. Fragmented files are slower to read than unfragmented files.

Free for all links page

Allows visitors to add links to any Web site onto the list, categorized by subject.

Friction (of war)

The aggregate of factors and events that reduce or degrade operational efficiency (and hence effectiveness) in the real world of war-making. The label is a metaphorical allusion to the heat loss that is an inescapable part of physical–mechanical systems.

FrontPage extensions

FrontPage is Microsoft's simple Web-page editor designed for nonprogrammers. It includes many of its own scripts and special effects, but to use them, you have to install the FrontPage "extensions" on your Web site. You should either plan to use CGI-based applications or

FrontPage. FrontPage does not provide the ability to edit or maintain files in your home directory and does not upload in true ASCII.

FTP account

Used to upload and download files to and from your Web site. You have unlimited access to your account 24 hours a day. You'll need to have FTP client software.

Global information environment

All individuals, organizations, or systems, most of which are outside the control of the military or national command authorities, that collect, process, and disseminate information to national and international audiences.

Guestbook

Visitors sign-in to your Web site, leaving a message to let you know what they thought of your site.

Hacker

The label "hacker" has come to connote a person who deliberately accesses and exploits computer and information systems to which he or she has no authorized access. Originally, the term was an accolade for someone highly motivated to explore what computers could do or the limits of his or her technical skills (especially in programming). "A great hack" was a common compliment for an especially cunning or innovative piece of software code. The term *cracker* was then reserved for people intruding into computer or information systems for the thrill of it (or worse). Over time, *cracker* faded from usage and *hacker* came to subsume its (unfortunate) connotations.

Head

A small electromagnetic device inside a drive that reads, writes, and erases data on the drive's media.

Heat Sink

A mass of metal attached to a chip carrier or socket for the purpose of dissipating heat.

Hijacking

A term (typically applied in combination with another) to connote an action to usurp activity or interactions in progress. Most commonly used for those tactics that allow an intruder to usurp an authorized user's session for his or her own ends.

History

(Internet browser) Stores the internet addresses (URLs) of the Web sites you have visited.

Hyperwar

A term (attributed to Air Force planners) describing the notion that war is becoming unimaginably and unmanageably fast.

I2WAR

Acronym for infrastructural and information warfare.

I/O Port

I/O stands for input/output. I/O is the communication between a computer and its user, its storage devices, other computers (via a network), or the outside world. The I/O port is the logical channel or channel endpoint in an I/O communication system.

I&W

Acronym for indications and warnings. This is a sort of catch-all label for any and all data signifying an operant or potential threat. Typically, indications and warnings connotes a summarization or fusion of raw data into a synopsis of current threat conditions (a report from an intel unit).

I&W/TA

Acronym for indications and warnings or threat assessment. This label is occasionally used to connote the summarization of incoming data with respect to threat conditions (extant or predicted).

IBW

Acronym for information-based warfare or intelligence-based warfare.

IDE

Stands for integrated drive electronics. Describes a hard disk with the disk controller integrated within it. See also "EIDE".

IDS

Acronym for intrusion detection system.

IDW

Acronym for information-dominance warfare.

IEW

Acronym for intelligence and electronic warfare.

Indications and warning(s) (I&W)

Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear or nonnuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to U.S. reconnaissance activities; terrorist attacks; and other similar events.

Indirect information warfare

Changing the adversary's information by creating phenomena that the adversary must then observe and analyze.

Industrial warfare

The class or character of war or warfare exemplified by the 18th century through to the present. Synonymous with second-wave warfare.

Information

Facts, data, or instructions in any medium or form. The meaning that a human assigns to data by means of the known conventions used in their representation. In intelligence usage, unevaluated material of every description that may be used in the production of intelligence.

Information Age

A label generally used to connote the present or prospective era in which information technology (IT) is the dominant technical artifact. The future time period when social, cultural, and economic patterns will reflect the decentralized, nonhierarchical flow of information; contrast this to the more centralized, hierarchical, social, cultural, and economic patterns that reflect the Industrial Age's mechanization of production systems.

Information Age warfare

That subset of war-making that uses information technology as a tool to impart combat operations with unprecedented economies of time and force. This is exemplified by a cruise missile on precision force projection.

Information attack

Directly corrupting information without visibly changing the physical entity within which it resides. In the wake of an information attack, an information function is indistinguishable from its original state except through inspecting its data or instructions.

Information-based warfare (IBW)

Synonym for information warfare. An approach to armed conflict focusing on managing and using information in all its forms and at all levels to achieve a decisive military advantage, especially in the joint and combined environment.

Information collection

That aspect of IW activities concerned with the acquisition of data. An organization needs a variety of information to support its operations. Information collection includes the entry points for information into an organization from both internal and external sources. Issues include quantity (completeness), quality (accuracy), and timeliness of this information. Business examples of collection systems include point-of-sale (POS) systems, market surveys, government statistics, and internal management data. Military examples of collection systems include tactical radars and other sensors.

Information compromise

That class or type of IW threat that involves a competitor gaining access to an organization's proprietary data.

Information denial

Measures beyond normal protection to specifically target an adversary's collection systems. There are two types of denial: direct attacks on the adversary's information systems, and providing misinformation to its systems to deceive and induce the adversary to take actions that are not to its advantage. For the military, direct attacks include electronic warfare (jamming) of sensors and radio links. Besides direct attacks, there are safer ways to corrupt an adversary's databases. These rely on providing false information to the targeted competitor's collection systems to induce this organization to make bad decisions based on this faulty information.

Information destruction

That class or type of IW threat to one's data assets that involves the loss of these data (or loss of access to these data) as the result of a hostile attack by an adversary.

Information dominance

In warfare, an operational advantage obtained through superior effectiveness of informational activity (acquisition and processing of data, information, and/or knowledge), to the extent that this advantage is demonstrated in practice through superior effectiveness of instrumental activity.

Information dominance warfare (IDW)

The subcategory of information warfare (IW) aimed at leveraging data, information, and knowledge to tactical and strategic advantage, as opposed to leveraging the media, channels, and vehicles of information transfer and processing. The goal of IDW is to achieve information dominance.

Information function

Any activity involving the acquisition, transmission, storage, or transformation of information.

Information in war (IinW)/information in warfare (IIW)

A term that has come to be used to denote the application of information (and information processing or technology) in the context of military operations (conventionally delineated), as opposed to that connotation accorded IW to the effect that information and information systems are the substance, the tools, and the targets in an emerging warform.

Information operations (also information ops)

This term is typically encountered in IW discussions as a label for those concrete tasks and activities by which one pursues one's own interests in the information realm. As such, information operations (or "info ops") most commonly denotes specific paths of action, in contrast to IW denoting the broader sphere within which these actions are undertaken.

Information ops (also "info ops")

Synonym for information operations.

Information protect (IP)
A (seemingly ungrammatical) synonym for information protection, quite frequently used in the U.S. military IW literature.

Information protection (IP)
Information protection addresses two types of threats: information compromise and destruction. Compromise involves a competitor gaining access to an organization's proprietary data. Destruction involves the loss of these data (or loss of access to these data) as the result of a hostile attack by an adversary.

Information realm
A commonly used term to denote the virtual space of data networks, contents, and commerce.

Information security (INFOSEC)
The protection of unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Information superiority
That degree of dominance in the information domain that permits the conduct of operations without effective opposition. Information superiority combines the capabilities of intelligence, surveillance, reconnaissance (ISR) and command, control, communications, computers, and intelligence (C4I) to acquire and assimilate information needed to effectively employ our own forces to dominate and neutralize adversary forces. It includes the capability for near-real-time awareness of the location and activity of friendly, adversary, and neutral forces throughout the battlespace and a seamless, robust C4I network linking all friendly forces that provides common awareness of the current situation.

Information system(s) (INFOSYS)
The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information systems security
A synonym for INFOSEC. Protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit and against the denial of service to authorized users.

Information systems warfare (ISW)
The subcategory of information warfare (IW) aimed at leveraging media, channels, and vehicles of information transfer and processing to tactical and strategic advantage.

Information terrorism
An ill-defined term (as yet) invoked to connote cyberspace mischief undertaken with intentions or ramifications analogous to the fear-inducing physical attacks one associates with terrorist activity.

Information transport
That element of IW activities that involves moving data from points of collection to points of storage or use. The speed with which this is done affects the timeliness of the data availability and, therefore, the responsiveness of the organization to situations. Transport considerations must be viewed within the overall IW perspective, because the same efficiency that facilitates rapid message and data transportation may also be used by a competitor to download proprietary databases in seconds or minutes.

Information war
Activities intertwined with, and superimposed on, other military operations, exploiting data and information in support of traditional military tasks such as command and control.

Information warfare (IW)

The broad class of activities aimed at leveraging data, information, and knowledge in support of military goals. Subcategories of information warfare can be differentiated into two general classes: (a) those aimed at leveraging the vehicles of information transfer or processing (information systems warfare [ISW]) and (b) those aimed at leveraging the informative content or effect of such systems.

IRQ

Stands for interrupt request. IRQ is the name of the hardware interrupt signals that PC peripherals (such as serial or parallel ports) use to get the processor's attention. Because interrupts usually cannot be shared, devices are assigned unique IRQ addresses that enable them to communicate with the processor. Peripherals that use interrupts include LAN adapters, sound boards, scanner interfaces, and SCSI adapters.

Java chat rooms

Real-time chat via a Java applet that allows visitors to your Web site to engage in live discussion with you or with each other. You can provide it just for fun or use it to interact with your customers in real-time.

Jumper

A small, plastic-covered metal clip that slips over two pins protruding from a circuit board. When in place, the jumper connects the pins electronically and closes the circuit, turning it on.

Kernel

An essential part of the operating system, responsible for resource allocation, low-level hardware interfaces, security, and more.

Key communicator

An individual or group having the economic, social, or political power to persuade the individuals or groups with which he or she interacts to change or reinforce existing opinions, emotions, attitudes, and behaviors.

Keystroke monitoring

A form of user surveillance in which the actual character-by-character traffic (that user's keystrokes) are monitored, analyzed, and logged for future reference. A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the host computer returns to the user.

Knowledge

The state or mechanism ascribed to a system to explain complex mediation between effective acquisition of data from, and effective action in, an operational environment. This approach to knowledge explicitly ties it to the processes of both education and inaction with respect to the given operational environment and hence links it to one or more specific actors in that given domain. These connections explain the IW literature's claims that knowledge is active and must be possessed if it is to exist— let alone be useful.

Knowledge-based warfare

The ability of one side to obtain essential and key elements of truth while denying these same elements of truth to the other side. The key attributes of knowledge-based warfare are timely, high fidelity, comprehensive, synthesized, and visual data. The end game is a complete pictorial representation of reality that the decision maker can tune to his or her unique needs at any given time. This picture must include both blue (one side) and red data (the other side), although this advanced concept technology demonstration (ACTD) concentrates on the provision of blue data only.

Knowledge dominance

In warfare, an operational advantage (vis-à-vis an adversary) in exploiting information to guide effective action. This is the goal of information dominance.

Knowledge war

A synonym for IW, or third-wave war.

Leapfrog attack

Any form of intrusion or attack accomplished by exploitation of data or information obtained on a site or server other than the attack's target.

Letter bomb/letterbomb

Malicious or disruptive code delivered via an email message (or an attachment to said message). A piece of email containing live data intended to do malicious things to the recipient's machine or terminal. Under UNIX, a letterbomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to tragic.

Logic bomb

The term for a mischievous or destructive piece of software (virus, trojan horse) that lies resident on the victim computer or system until triggered by a specific event (onset of a predetermined date or set of system conditions).

Lost cluster chain

A cluster on disk that is not registered as free but does not have any known data in it.

Mail bomb/mailbomb

Unlike a logic bomb (a thing), mail bomb is a verb used to connote deliberately deluging a target system or host with email messages for purposes of harassment, degradation of service, or even denial of service.

Mail storm/mailstorm

What the target system or users see when being mail bombed. Any large amount of incoming email sufficient to disrupt or bog down normal local operations. What often happens when a machine with an Internet connection and active users reconnects after extended downtime—a flood of incoming mail that brings the machine to its knees.

Majordomo list

This is a very flexible tool for allowing your clients to interact with each other by email. In simple terms, it is an interactive email discussion group that allows all subscribers to send and receive messages to and from everyone on the list through email, sort of like an email chat room, but not in real-time. Majordomo lists usually focus on a particular topic of common interest, such as dried flower arranging, forensics, or anything that people can share information or talk about. There are many configurable features including automatic subscribe and unsubscribe. Each list can email up to 1,500 emails per day.

MASINT

Acronym for measurement and signature intelligence.

Measurement and signature intelligence

Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and measurement of the same.

MEII

Acronym for minimum essential information infrastructure.

Message

Any thought or idea expressed briefly in a plain or secret language and prepared in a form suitable for transmission by any means of communication.

MIE

Acronym for military information environment.

Military deception

Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

Military information environment (MIE)

The environment contained within the global information environment, consisting of information systems and organizations (friendly and adversary, military and nonmilitary) that support, enable, or significantly influence a specific military operation.

Military information function

Any information function supporting and enhancing the employment of military forces.

Military technical revolution (MTR)

A term from Soviet military theory of the late 1970s. It denotes the phenomenon of extreme transformations in warfare occurring as a result of the exploitation of technology. The Soviets saw the operational and organizational innovations resulting from the exploitation of the technology as defining a military technical revolution.

Minimum essential information infrastructure (MEII)

A label for the least set of own-force information assets that can serve to support a given mission or operation.

Mirror image backups

Also referred to as bit-stream backups, these involve the back up of all areas of a computer hard disk drive or other type of storage media (Zip disks, Jaz disks, etc.). Mirror image backups exactly replicate all sectors on a given storage device. Thus, all files and ambient data storage areas are copied. Such backups are sometimes referred to as "evidence grade backups" and they differ substantially from standard file backups and network server backups.

Misuse detection

The class of intrusion detection tactics that proceed on the presumption that problematical intrusions (attacks) can be positively characterized and that detection of their characteristic profile is sufficient for identifying potential threats.

Mockingbird

A computer program or process that mimics the legitimate behavior of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user.

Monthly traffic (bandwidth)

The sum of outward-bound or inward-bound Web pages, files, email, and anonymous FTP traffic. Each time a Web page, image, audio, video, or other element of your Web site is accessed by your visitor, traffic is generated.

Motherboard

The "heart" of your PC—it handles system resources (IRQ lines, DMA channels, I/O locations), as well as core components such as the CPU and all system memory. It accepts expansion devices such as sound and network cards and modems.

mSQL database

A database engine used for accessing individual records.

MTR

Acronym for military technical revolution.

National information infrastructure (NII)

A general label for the composite network of data or information systems and connectivity channels that serve as the foundation for U.S. economic, political, and military operations.

Navigation warfare (NAVWAR)

A term for activities directed toward disrupting, degrading, or denying the adversary's capabilities for geographical location, tracking, and control (navigation) based on such capabilities. This term is currently used specifically to connote those EW and IW (and counter-EW and -IW) measures involving the global positioning system (GPS) network of satellites and terrestrial, airborne, or shipborne receivers.

Netwar

A synonym for cyberwar.

Network spoofing

In network spoofing, a system presents itself to the network as though it were a different system (system A impersonates system B by sending B's address instead of its own). The reason for doing this is that systems tend to operate within a group of other "trusted" systems. Trust is imparted in a one-to-one fashion; system A trusts system B (this does not imply that system B trusts system A). Implied with this trust is that the system administrator of the trusted system is performing his or her job properly and maintaining an appropriate level of security for his or her system. Network spoofing occurs in the following manner: if system A trusts system B and system C spoofs (impersonates) system B, then system C can gain otherwise denied access to system A.

Network worm

A worm that migrates across platforms over a network by copying itself from one system to another by exploiting common network facilities, resulting in execution of the (replicated) worm on that system and potentially others.

NII

Acronym for National Information Infrastructure.

NTFS

Windows NT file system.

Offensive counterinformation

Actions against the adversary's information functions.

OODA loop (also O-O-D-A loop)

Observation, orientation, decision, action loop. Taken to describe a single iteration of the cycle proceeding from data acquisition, through information integration and decision making, to inaction of a response. Disruption or other damage to the OODA loop is a common way of portraying the goal or main effect of IW.

OOTW

Acronym for operations other than war (missions carried out by the military that lie outside the scope of what is conventionally termed "war"). Examples include humanitarian and police actions.

Open-source intelligence (OSINT)

Information of potential intelligence value that is available to the general public.

Operational intelligence

Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations.

Operations security (OPSEC)

A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities.

Opinion

A view, judgment, or appraisal formed in the mind about a particular matter or particular matters. It may also be said to be an intellectually defined judgment of what is true for the individual or group. It may be more influenced by attitudes than facts.

Orientation

An interactive process of many-sided implicit cross-referencing projections, empathies, correlations, and rejections that shapes and is shaped by the interplay of genetic heritage, cultural tradition, previous experiences, and unfolding circumstances.

OSINT

Acronym for open-source intelligence.

Packet sniffer

A device or program that monitors the data traveling between computers on a network.

Packet sniffing

Packet sniffing is a technique in which attackers surreptitiously insert a software program at remote network switches or host computers. The program monitors information packets as they are sent through networks and sends a copy of the information retrieved to the hacker. By picking up the first 125 keystrokes of a connection, attackers can learn passwords and user identifications, which, in turn, they can use to break into systems.

Partition

A logical section of a disk. Each partition normally has its own file system.

Partition table

A 64-byte data structure that defines the way a PC's hard disk is divided into logical sectors known as partitions. The partition table describes to the operating system how the hard disk is divided. Each partition on a disk has a corresponding entry in the partition table. The partition table is always stored in the first physical sector of a disk drive.

Passive attack

A form of attack in which data is released (captured or obtained) from the target system. Attack that does not result in an unauthorized state change, such as an attack that only monitors or records data.

Passive threat

The threat of unauthorized disclosure of information without changing the state of the system. A type of threat that involves the interception, not the alteration, of information.

Password cracking/password theft

Password cracking is a technique used to surreptitiously gain system access by using another user's account. Users often select weak passwords. The two major sources of weakness in passwords are easily guessed passwords based on knowledge of the user (for example, wife's maiden name) and passwords that are susceptible to dictionary attacks (brute-force guessing of passwords using a dictionary as the source of guesses). Password cracking and theft is a technique in which attackers try to guess or steal passwords to obtain access to computer systems. Attackers have automated this technique; rather than attackers trying to guess legitimate users' passwords, computers can very efficiently and systematically do the guessing. For example, if the password is a dictionary word, a computer can quickly look up all possibilities to find a match. Complex passwords comprised of alphanumeric characters are more difficult to crack. However, even with complex passwords, powerful computers can use brute force to compare all possible combinations of characters until a match is found.

Password sniffing

A form of sniffing that entails sampling specific portions of the data stream during a session (collecting a certain number of initial bytes where the password can be intercepted in unencrypted form on common Internet services) so as to obtain password data that can then be exploited.

Path

A location of a file. The path consists of directory or folder names, beginning with the highest-level directory or disk name and ending with the lowest-level directory name. A path can identify a drive (C:\), a folder (C:\Temp), or a file (C:\Windows\ftp.exe).

Penetration

With regard to IW, a successful attack—the ability to obtain unauthorized (undetected) access to files and programs or the control state of a computer system.

Penetration signature

The description of a situation or set of conditions in which a penetration could occur or of system events that in conjunction can indicate the occurrence of a penetration in progress.

Perception

The process of evaluating information that has been received and classified by the five physical senses (vision, hearing, smell, taste, and touch) and interpreted by criteria of the culture and society.

Perception management

Actions to convey and deny selected information and indicators (1) to foreign audiences to influence their emotions, motives, and objective reasoning and (2) to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations.

Peripheral

Any part of a computer other than the CPU or working memory (RAM and ROM). For example, disks, keyboards, monitors, mice, printers, scanners, tape drives, microphones, speakers, and other such devices are peripherals.

Phracker

Individual who combines phone phreaking with computer hacking. Formed by a play on both *phreaker* and *hacker*.

Phreak/phone phreak

A term for hacking or cracking-type exploitation directed at the telephone system (as opposed to the data communications networks). When the intrusion or action involves both telephone and data communications networks, that portion of the intrusion activity directed toward manipulating the telephone system is typically called phreaking.

Phreaker

Individual fascinated by the telephone system. Commonly, an individual who uses his or her knowledge of the telephone system to make calls at the expense of another.

Plug-and-Play (PnP)

A hardware and software specification developed by Intel that allows a PnP system and a PnP adapter to configure automatically. PnP cards generally have no switches or jumpers but are configured via the PnP system's BIOS or with supplied software for non-PnP computers.

POST

Stands for power-on self test. Each time a PC initializes, the BIOS executes a series of tests collectively known as the POST. The test checks each of the primary areas of the system, including the motherboard, video system, drive system, and keyboard, and ensures that all components can be used safely. If a fault is detected, the POST reports it as an audible series of beeps or a hexadecimal code written to an I/O port.

RAM

Random zccess memory (see also "DRAM," "SDRAM"). A data-storage device for which the order of access to different locations does not affect the speed of access. This is in contrast to magnetic disk or magnetic tape, where it is much quicker to access data sequentially because accessing a nonsequential location requires physical movement of the storage medium rather than just electronic switching.

The most common form of RAM in use today is built from semiconductor integrated circuits, which can either be static (SRAM) or dynamic (DRAM).

Random text displayer

Visitors see random messages you have saved in a text file, such as famous quotes or announcements. Generally, the visitor will see a different message every time they visit the site.

Raw stats/graphic stats/advanced stats

You have access to a raw access log so you can analyze your site's usage with any program you desire. Graphical stats are a detailed graphical and tabular view of your Web site's traffic grouped by weeks, days, and hours in an easy to read format.

Real Audio/Video

A client–server based system where both the browser and server must have real audio/video components to provide streaming media to visitors at a Web site without waiting for the clip to download.

Retro-virus

A virus that waits until all possible backup media are also infected, so that it is not possible to restore the system to an uninfected state.

Revolution in Military Affairs (RMA)

Current term for the transformations driven by the proliferation of information technology (IT) as tools for optimizing military operations and weapons of military utility. The current RMA is an instance of a military technical revolution (MTR).

Right-click

To right-click an item is to point to it with the screen pointer and then quickly press and release the right mouse button once.

Risk

With specific regard to data or information systems—accidental or unpredictable exposure of information, or violation of operations integrity because of the malfunction of hardware or incomplete or incorrect software design.

RMA

Acronym for revolution in military affairs.

ROM

Read-only memory. A type of data-storage device that is manufactured with fixed contents. The term is most often applied to semiconductor-integrated circuit memories. ROM is inherently nonvolatile storage—it retains its contents even when the power is switched off, in contrast to RAM. It is used in part for storage of the lowest level bootstrap software (firmware) in a computer.

SA

Acronym for situation awareness.

Scavenge/scavenging

Searching through object residue (discarded disks, tapes, or paper) to acquire sensitive data without authorization.

Scripts

Scripts are programs written to run with Web pages and perform a specific task in response to visitor actions such as clicking a button. For example, a Perl script counts the visits to the page, and a JavaScript script makes the buttons change colors when you put your mouse pointer over them. Scripts can be written in Perl, Java, JavaScript, VBScript, and a dozen other programming languages.

SCSI

Stands for small computer system interface. A standard that allows multiple devices to be connected in daisy-chain fashion.

SDRAM

Stands for synchronous dynamic random access memory (see also "DRAM"). SDRAM incorporates new features that make it faster than standard DRAM and EDO memory.

Search engine

A CGI script that allows visitors to perform keyword searches of a Web site.

Second-wave war(fare)

A synonym for industrial warfare—the mode of warfare characteristic of nation states as they developed during the Enlightenment, through the Industrial Revolution, and through the 20th century.

Sector

The tracks on a disk are divided into sectors. Clusters contains from 1 to 64 sectors.

Secure server (SSL)

One method of ensuring that information entered through your Web site is protected. Information submitted via a secure form is sent to the server in encrypted mode. This is most commonly used for credit card transactions.

Security

Measures taken by a military unit, an activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness.

Security audit

A search through a computer system for security problems and vulnerabilities.

Security breach

A violation of controls of a particular information system such that information assets or system components are unduly exposed.

Security classification

A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required.

Select

To select an item is to identify to the computer one or more files or folders that you wish to do something with. This is usually done by pointing to an item with the screen pointer and then quickly pressing and releasing the left mouse button once.

Sensor-to-shooter

A descriptive phrase employed to connote the cumulative feed-forward of data and information through an operational military system, from initial acquisition of novel data elements (via the sensors) through to the element effecting instrumental response as needed (the shooter). A loose descriptor for the scope of processing for intrasystemic functions to obtain advantage in a theater of operations.

Server

A special computer designed for the Internet or another network, usually far more powerful than a regular desktop computer, that has a full-time direct connection to the Internet. Some servers even have two or more processors working together. Servers run special software called Web server software, which enables them to receive requests and deliver files to other computers across the Internet.

Server side includes (SSI)

Allows the server to understand and respond to special page commands. As an example, if you had a footer you wanted on all your pages that may change from time to time, you can create a text file with the desired footer and place it in your document. On each page you put a simple include to read the file and place it at the bottom of the desired pages. Changing the footer on all your pages would be as simple as changing the one text file.

Session hijacking

Taking over an authorized user's terminal session, either physically when the user leaves his or her terminal unattended or electronically when the intruder carefully connects to a just-disconnected communications line.

Shared situation awareness (SSA)

The collective perception, comprehension, and projection of environmental elements among a set of actors.

Shopping cart

Keeps track of what your customers have ordered online as they add and remove items. When a customer is ready to check out, the program tallies the order for processing and takes their credit card and other information.

SIGINT

Acronym for signals intelligence.

Signal

As applied to electronics, any transmitted electrical impulse.

Signal security (SIGSEC)

A generic term that includes both communications security and electronic security.

Signals intelligence (SIGINT)

A category of intelligence composed of—either individually or in combination—all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

SIGSEC

Acronym for signal security.

Simple counter

Graphical count of visitors to your Web site, which appears on your Web page.

Site submission

Submits your site information to a database of over 1,900 search engines, link engines, and directories.

Situation awareness (SA)

Sometimes termed "situational awareness." The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. This term is broadly used to denote the state of awareness that a subject (operator, pilot) has in the course of a task at a given point in time. As such, it connotes a degree of orientation to those circumstances at that point in time—particularly those that are germane to the task itself. The term is also (more loosely) used to connote such a state of awareness or orientation with respect to multiple actors or organizational units. As such, the notion of situation awareness maps straightforwardly onto the orientation phase of the OODA Loop.

Slot

A physical connector on a motherboard to hold an expansion card, SIMM, DIMM, or a processor card in place.

Sniff/sniffing

The act of surreptitiously monitoring data streams so as to intercept and capture exploitable information.

Sniffer

A tool used to intercept potentially exploitable data from the traffic on a network. A program to capture data across a computer network. Used by hackers to capture user-ID names and passwords. A software tool that audits and identifies network traffic packets.

Social engineering

A term for personal (social) tactics employed in support of attempts to achieve unauthorized access to a computer or information system. This is something of a catch-all category for any tricks used to obtain the intended access or to obtain information critical to achieving that access.

Socket

A receptacle, usually on a motherboard, that processors or chips can be inserted into.

SOS

Acronym for system of systems.

Spam

The act of bombarding a target (system, Usenet news group, set of email addresses) with sufficient volume of data (or a volume of sufficiently massive data items) such that degradation or even denial of service is achieved. This term is also pejoratively applied to describe the perceived harassment of receiving profligately broadcast data (junk email advertising). To crash a program by overrunning a fixed-site buffer with an excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

Spectrum management

Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

System registry

The system configuration files used by Windows 2000, XP, 2003, and NT to store settings about user preferences, installed software, hardware and drivers, and other settings required for Windows to run correctly. The system updates the registry every time you add new hardware or a new program to your system. When the registry becomes "broken," it can cause serious system problems.

Tactical internet

A battlefield communication system networked together using commercially based internet protocols.

TECHINT

Acronym for technical intelligence.

Technical attack

An attack that can be perpetrated by circumventing or nullifying hardware and software protection mechanisms, rather than by subverting system personnel or other users.

Technical intelligence (TECHINT)

Intelligence derived from exploitation of foreign materiel, produced for strategic, operational, and tactical level commanders. Technical intelligence begins when an individual service member finds something new on the battlefield and takes the proper steps to report it. The item is then exploited at succeedingly higher levels until a countermeasure is produced to neutralize the adversary's technological advantage.

Telnet account

Telnet allows real-time access to the command line of your server to run programs and install and configure scripts. Most CGI scripts can be installed without Telnet unless you need it for debugging purposes.

Terminal hijacking

Allows an attacker on a certain machine to control any terminal session that is in progress. An attack hacker can send and receive terminal I/O while a user is on the terminal.

Terminator

Most commonly found in relation to a SCSI chain, this prevents the reflection or echoing of signals that reach the ends of the SCSI bus. Usually terminators are hardware circuits or jumpers.

Third-wave war(fare)

A synonym for IW or knowledge war. The allusion is to Toffler's "Third Wave" of economic activity, which concentrates on information and knowledge as raw material and product. This three-tiered economic or political model was a major influence on the DoD thinkers whose work led to today's interest in IW.

Time bomb

A logic bomb that is specifically triggered by a temporal event (a predetermined date or time). A logic bomb that is triggered by reaching some preset time, either once or periodically. A variant of the trojan horse, in which malicious code is inserted to be triggered later.

TRANSEC

Acronym for transmission security (communications security).

Trap door

A hidden software or hardware mechanism used to circumvent security control.

Trojan horse

An independent program that, when called by an authorized user, performs a useful function but also performs unauthorized functions, often usurping the privileges of the user.

Troll

To subvert a forum by deliberately posting provocative (especially provocatively stupid) messages with the intention of distracting others into response.

Unallocated file space

Unallocated file space and file slack are both important sources of leads for the computer forensics investigator. The data-storage area in a factory-fresh hard disk drive typically contains patterns of sectors that are filled with patterns of format characters. The same format pattern is sometimes used in the format of hard disk drives, but the format patterns can consist of essentially any repeat character as determined by the factory test machine that made the last writes to the hard disk drive. The format pattern is overwritten as files and subdirectories are written in the data area.

Unzip

To unzip is to extract (see "Extract") a Zip archive.

UUencode

Many file formats are 8-bit (also called binary), which means the basic unit of information—a byte—comprises 8 on/off signals. Email, however, is a 7-bit (or text) medium, preventing the transfer of 8-bit data. UUencoding compensates for this restriction by converting 8-bit data to 7-bit data. UUencode accomplishes this by joining all of the file's bits together into a single stream and then dividing the stream into 7-bit chunks. The data are then emailed and received by someone who must UUdecode it.

Vandal

As contrasted with crackers and criminals in a tripartite taxonomy of cyberspace intruders, this term is used to denote anyone whose goal is to destroy information and information systems in the course of their intrusion attempts.

Video adapter

An expansion card or chip set built into a motherboard that provides the capability to display text and graphics on the computer's monitor. If the adapter is part of an expansion card, it also includes the physical connector for the monitor cable. If it is a chip set on the motherboard, the video connector will be on the motherboard also.

Virtual battlespace

The ether occupied by communications impulses, databases, and computer codes. In this usage, the term is synonymous with cyber medium, cyberspace, and infosphere.

Virtual realm

A synonym for information realm or cyberspace.

Virus

The generic label for a unary set of code that is designed to cause mischief or other subversive effect in a target computer system.

Vulnerability

With specific regard to IW—a known or suspected flaw in the hardware or software or operation of a system that exposes the system to penetration or its information to accidental disclosure.

War

An event characterized by the open, total, and (relatively) unrestricted prosecution of warfare by lethal means. As such, war is not synonymous with warfare.

War dialer

A cracking tool, a program that calls a given list or range of numbers and records those that answer with handshake tones (and so might be entry points to computer or telecommunications systems).

Warfare

The set of all lethal and nonlethal activities undertaken to subdue the hostile will of an adversary or enemy. The distinction between this and war ties into the delineation of information warfare as an activity, which could or should be conducted outside the situational frame of war itself.

Warm boot

Rebooting a system by means of a software command as opposed to turning the power off and on. See also "Cold boot."

Web-based Telnet

Invoke a telnet session directly from your Web browser. There's no need for any other applications or software.

Windows swap files

Windows swap files are relied on by Windows, Windows 2000, Windows XP, and Windows 2003 to create "virtual memory" (using a portion of the hard disk drive for memory operations). The storage area is important to the computer forensics specialist for the same reason that file slack and unallocated space are important (large volumes of data exist for which the computer user likely has no knowledge). Windows swap files can be temporary or permanent, depending on the version of Windows involved and settings selected by the computer user. Permanent swap files are of more interest to a computer forensics specialist because they normally store larger amounts of information for much longer periods of time.

Wizard

A wizard is a series of dialog boxes that guides you step by step through a procedure.

World Wide Web

The World Wide Web, or WWW, is the part of the Internet that you use to view a particular Web page. The Web is just a set of protocols, or standards, for transferring data from one computer to another; just one aspect of the Internet, but by far the most popular. Telnet, FTP, Veronica, and Archie are some other Internet data-transfer protocols. Without protocols, computers wouldn't be able to communicate with or understand each other.

Worm

A class of mischievous or disruptive software whose negative effect is primarily realized through rampant proliferation (via replication and distribution of the worm's own code). Replication is the hallmark of the worm. Worm code is relatively host-independent, in that the code is self-contained enough to migrate across multiple instances of a given platform, or across multiple platforms over a network (network worm). To replicate itself, a worm needs to spawn a process; this implies that worms require a multitasking operating system to thrive. A program or executable code module that resides in distributed systems or networks. It will replicate itself, if necessary, in order to exercise as much of the systems' resources as possible for its own processing. Such resources may take the form of CPU time, I/O channels, or system memory. It will replicate itself from machine to machine across network connections, often clogging networks and computer systems as it spreads.

Zip

To zip (notice the lower case z) a file is to compress it into an archive so that it occupies less disk space.

Zip archive

An archive of one or more Zip-compressed files. When used as a noun, Zip is typically capitalized. Compressed files can come in many formats besides Zip.

Zip file

A Zip archive that Windows presents as a single file. In general, the contents cannot be accessed unless the archive is decompressed.

Index