Cyber Attacks
A General Look

- Organizational Background
- Cyber Attacks Overview
- Terrorist Groups Cyber Capabilities
- Questions

Terrorism: Background

- The threat of terrorist attacks against Indian citizens and India interests around the world has become the Nation's principal national security issue
- The cyber security of the India is of paramount importance

The Washington Times

For home delivery, call
202-636-3333

SITE SEARCH | CLASSIFIEDS | ARCHIVES | SUBSCRIBE | CONTACT US | ABOUT TWT

SEARCH

DAILY
Front Page
Nation/Politics
World
Commentary
Opinion/Editorial
Metropolitan
Sports
Business
Technology
Entertainment
Culture
Weather

WEEKLY
Business Times
Family Times
Auto Weekend
Wash. Weekend
Books
Home Guide
Arts
Nat'l Weekly Edition

MARKETPLACE
Classifieds

January 31, 2002

Nuclear plants targeted

By Bill Gertz
THE WASHINGTON TIMES

U.S. intelligence agencies have issued an internal alert that Islamic terrorists are planning another spectacular attack to rival those carried out on September 11.

The detailed warning was issued within the past two weeks in a classified report that said one target was a U.S. nuclear power plant or one of the Energy Department's nuclear facilities.

The alert was based on sensitive intelligence gathered overseas that revealed discussions among terrorism suspects.

The latest warning was similar to other terrorist threats that prompted

Top Stories
- Bush unveils $2.13 trillion budget
- U.S.: Iran aids terrorists' flight
- Body is not Pearl's, say police
- How much metal should be in a Medal of Honor?
- Now that one was a

Cyber Attacks

- The Prussian philosopher Karl von Clauswitz observed: "*Every age has its own kind of war, its own limiting conditions and its own peculiar preconceptions.*"
- We live in an age of TECHNOLOGY focused warfare

Definition

- Cyber Attacks: computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or information resident on it

Lessons From Past Cyber Attacks

- Cyber attacks accompany physical attacks
- Cyber attacks are increasing in volume, sophistication, and coordination
- Cyber attacks are attracted to high-value targets

Physical Conflicts and Cyber Attacks

- The Pakistan/India Conflict
- The Israel/Palestinian Conflict
- The Former Republic of Yugoslavia (FRY)/NATO Conflict in Kosovo
- The U.S. – China Surveillance Plane Incident

Potential Cyber Attacks

- Unauthorized Intrusions
- Defacements
- Domain Name Server Attacks
- Distributed Denial of Service Attacks
- Computer Worms
- Routing Operations
- Critical Infrastructures
- Compound Attacks

washingtonpost.com

Root-Server Attack Traced to South Korea, U.S.

By Brian Krebs
washingtonpost.com Staff Writer
Thursday, October 31, 2002; 3:30 PM

Last week's attacks on the Internet's backbone likely emanated from computers in the Unite

"The investigation is ongoing," Mueller said at an Internet security conference in Falls Church

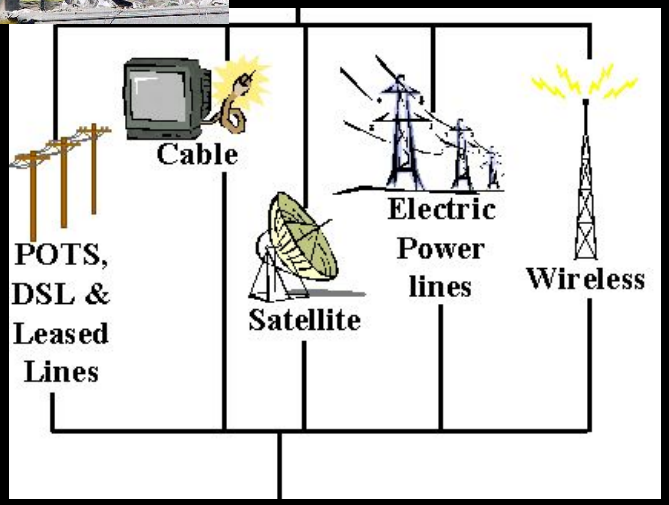
Last Monday, a distributed denial of service (DDOS) attack struck the 13 "root" servers tha
Internet domains like dot-com and dot-info.

East Asia is a major source of cyber crime and computer attacks, in part because of the relat
hackers use dozens -- and often hundreds -- of commandeered computers to overwhelm tar
more broadband connections per capita than any other country.

"We've tracked a total of at least 80,000 zombie machines in South Korea that are trivially e
tracks the source and type of cyberattacks worldwide. "These are machines that have ready-

According to several recent studies, only the United States surpasses South Korea as an orig

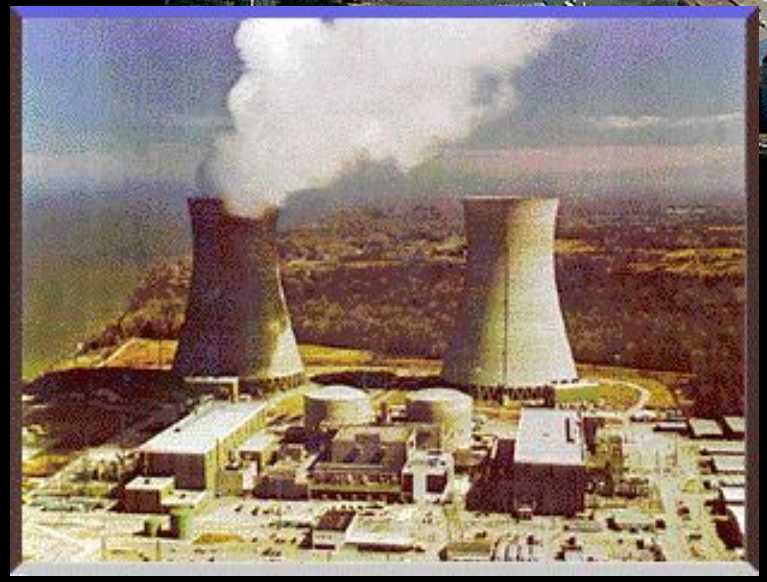
Compound Attacks



- Employ some or all of aforementioned cyber attacks
- Possibly combined with conventional (physical) terror attack
- Consequences include devastating disruption in communication and commerce

Critical Infrastructures

- Critical infrastructures include gas, power, water, banking and finance, transportation, communications
- All dependent to some degree on information systems
- Insider threat - specialized skills



Cyber warfare & Terrorism

- Cyber warfare
- Cyberwarfare utilizes techniques of defending and attacking information
- Cyber Terrorism
- Cyberterrorism, is "the use of computer network tools to shut down critical national infrastructures

Factors of cyber attacks against a group

- Fear factor
  - create fear amongst individuals, groups, or societies
- Spectacular factor
  - it is the actual damage of the attack
- Vulnerability factor
  - exploits how vulnerable an organization or government establishment is to cyber-attacks

Potential Sources of Attacks

1. Thrill Seekers
2. Terrorist Sympathizers and Anti-national Hackers
3. Terrorist Groups
4. Nation-States


NEWSBYTES®

HOME | SEARCH | Telecom | E-Commerce | Computers | Web Site Reviews

Pakistani Group Strikes U.S. Military Web Site

By Brian McWilliams, Newsbytes
POINT MUGU, CALIFORNIA, U.S.A.,
21 Oct 2001, 1:01 PM CST

Delivering on earlier threats, a Pakistani hacking group defaced
site operated by the U.S. Department of Defense on Saturday


MPUTER WEEK | GOVERNMENT E-BUSINESS | TECHNOLOGY | EVENTS | LINKS | DI

Federal Computer Week

Al Qaeda cyber alarm sounded

BY William Matthews
July 25, 2002

Printing? Use this version
Email this to a friend

There is a 50 percent chance that the next time al Qaeda terrorists strike the United States, their attack will include a cyberattack, Rep. Lamar Smith (R-Texas) warned.

RELATED LINKS

"Infosec research bill amended" [FCW.com, May 21, 2002]

Terrorist Groups

- Terrorist groups are using information technology
- Terrorists possess the will and may easily obtain the means to attack IT targets
- Potential for targeted cyber attacks is growing

Terrorist Cyber Capabilities

- What information technologies are terrorist groups using?

Terrorist Cyber Capabilities

1. Propaganda
2. Recruitment & Training
3. Fundraising
4. Communications
5. Targeting

1. Cyber Capabilities: Propaganda

- High level use for disseminating ideology and building nationalistic vision
- English and Arabic web sites
- Toned down English sites often lead to more radical materials (ex: encyclopedia for the Jihad)

1. Cyber Capabilities: Propaganda

- Alneda.com
- Azzam.com

Agents Pursue Terrorists Online

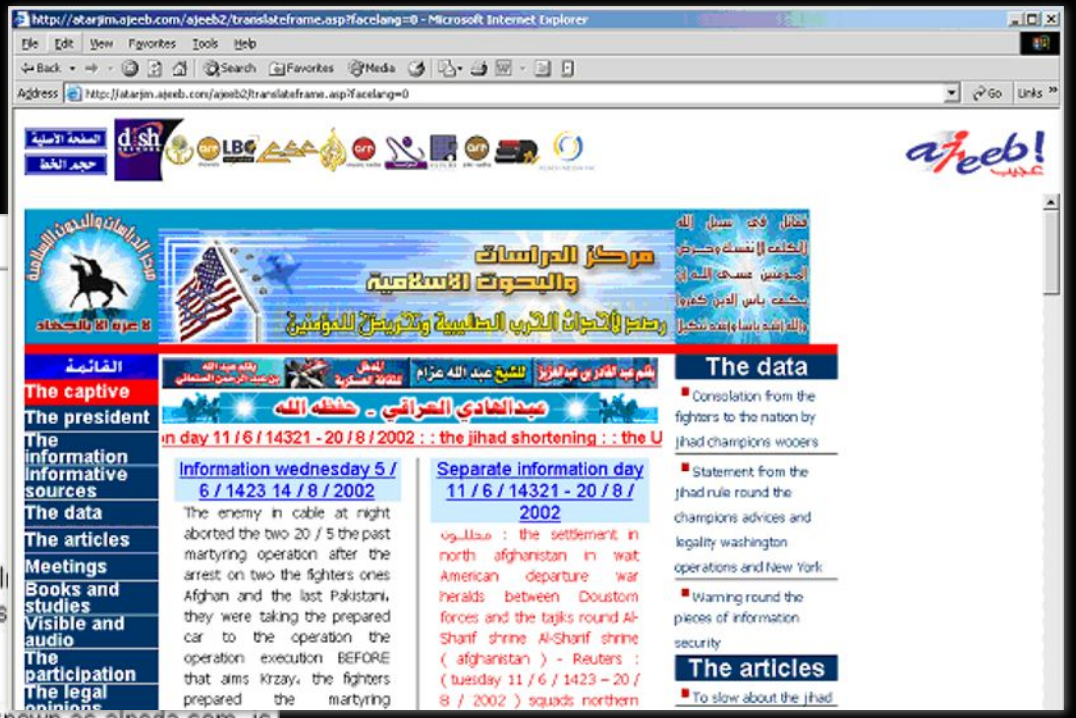
By Jack Kelley
June 21, 2002
http://www.newsfactor.com/perl/story/18331.html

U.S. officials are searching the I
used by al-Qaeda to deliver mes
operatives around the world.

The Arabic Web site, recently known as alneda.com, is
of the terrorist group's main instruments in its effort to re
here say.

According to one analyst, al-Qaeda leaders prefer to use a Web site to communicate with followers, rather than telephones or mass e-mails that are much easier to trace.

The site, which is registered in Singapore, appeared on
before it was taken off at the request of U.S. officials. Th
numerical address in an effort to throw off FBI and CIA s



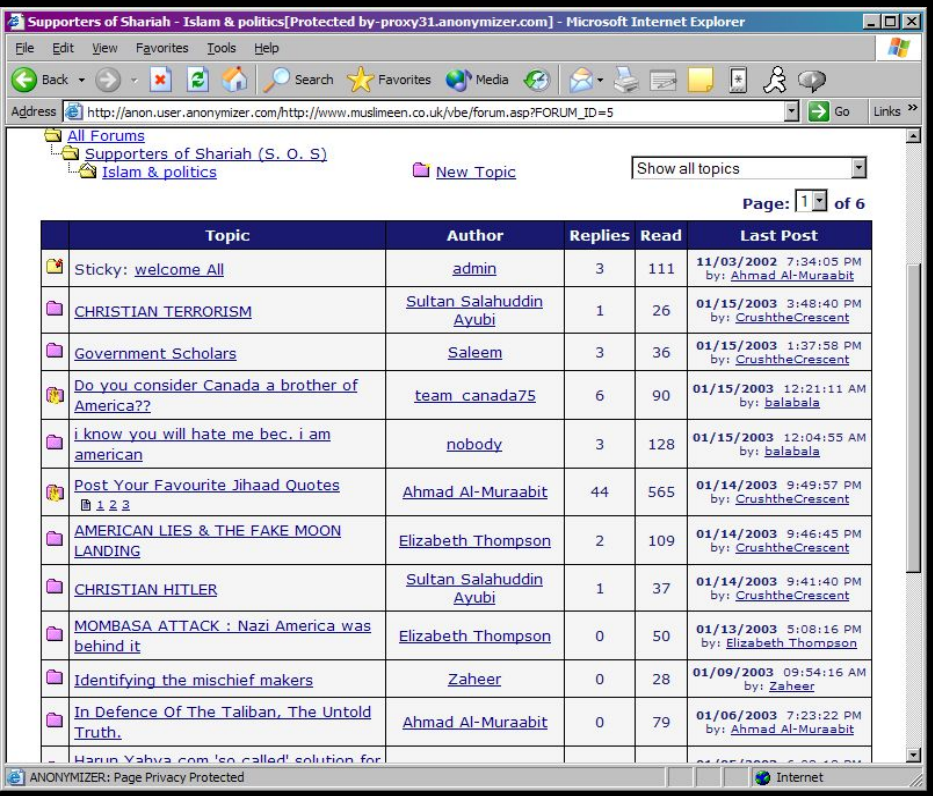
Propaganda: Analysis

- Provide news and information with a fundamentalist spin
- religious and military leaders tell their story
- Rulings on legal and religious matters
- Photos of alleged atrocities
- Links to other sympathizer sites
- Many are in Arabic-only

2. Cyber Capabilities: Recruitment & Training

- Lengthy rationales from religious leaders on why jihad not just allowed, but necessary
- "Interviews with jihadi in the field, battle accounts
- Poetry glorifying acts, leaders and rationale
- Videos

2. Cyber Capabilities: Recruitment & Training

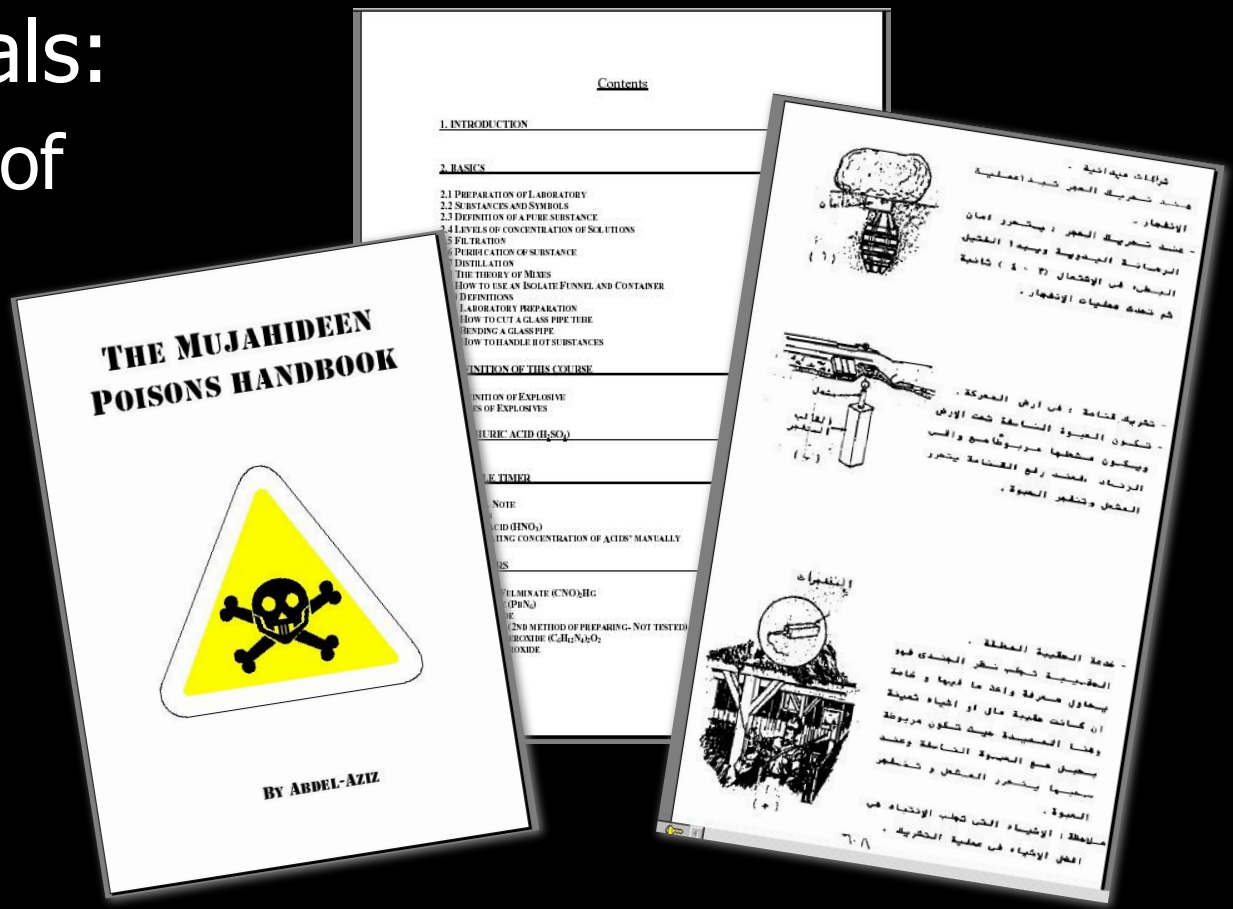


Message boards

- Online forums for exchanging info, debate, proselytizing
- Downloadable videos of fighting in Chechnya, Afghanistan, Kurdistan
- Audio and video files of UBL, Zawarhi, Sulaiman Abu Ghaith, and others

2. Cyber Capabilities: Recruitment & Training

- How-to manuals:
  - Encyclopedia of Jihad
  - Bombs and Explosives
  - Chemicals
  - Kidnapping
  - Assassination
  - Poisons



Recruitment & Training: Analysis

- Websites used for propaganda are often set up to recruit as well
  - Use of photos, interviews, and video footage common
- How to manuals readily available
- Message board used for communications
- Highly technical operatives have and continue to play key roles in Terrorist organizations

3. Fundraising: Examples

2001: Somalia Internet Company

- Source of either funding or money laundering for al-Qaeda

2002: Infocom

- Legitimate activities hiding channeling of funds?
- Dallas: Elashi brothers all indicted
- Accused of export violations (computers and peripherals to Libya, Syria)
- Accused of money laundering for Hamas

3. Fundraising: Examples

Benevolence International Foundation (BIF)

- April 2000, BIF wire transferred ~$700K to bank accounts tied to Chechen mujahideen
- Indicted on Federal perjury, racketeering charges in 2002
- Prosecutors: knowingly diverted donations to terrorists including AQ
- Enaam Arnaout plead guilty to one count of racketeering conspiracy related to directing BIF donations to purchase clothing and equipment for "fighters" in Bosnia and Chechnya

Fundraising: Analysis

- Radical news sites often take online donations
- terrorist groups understand how to raise funds over the internet
- Examples of credit card fraud and other crimes used to fund or facilitate terrorist groups will continue to grow

4. Cyber Capabilities: Comms & Security

- Bin Laden's phone number from International Maritime Satellite 873682505331
- Encryption
  - Operatives are trained on up to date encryption techniques and software
  - Terrorist training manuals
  - Terrorist training camps
  - Sept 11 use - email
  - Many computers found in Afghanistan contained encrypted data

4. Cyber Capabilities: Comms & Security

- Secure Communications
- Steganography
  - Many reports in the media of the use of this technology
  - Over 100 tools readily available
  - The problem lies in detecting the use of the technology – and reading it

Communications: Analysis

- terrorists are communicating over the internet
- Beyond email and message boards there is evidence that terrorist groups are using encryption to secure their communications
- Advanced data hiding and communication security tools are readily available and may be in use by terrorist organizations

5. Cyber Capabilities: Targeting

- Cost benefit analysis
  - A terrorist studies a target's defensive capabilities much the same way special operations forces target objectives.
  - Key operative in the African embassy bombings, Ali Abdelseoud Mohamed, actually served with the U.S. Army Special Forces.

5. Cyber Capabilities: Targeting

- East African embassy bombings

  "Prior to carrying out the operation, Al-Qaeda conducts surveillance of the target, sometimes on multiple occasions, often using nationals of the target they are surveilling to enter the location without suspicion. The results of the surveillance are forwarded to Al-Qaeda HQ as elaborate "ops plans" or "targeting packages" prepared using photographs, CADCAM (computer assisted design/computer assisted mapping) software, and the operative's notes."

J.T. Caruso, Acting Assistant Director, FBI Counterterrorism Division
before Senate Committee on Foreign Relations Subcommittee on International Operations and Terrorism,
12/18/01, http://www.fbi.gov/congress/congress01/caruso121801.htm

5. Cyber Capabilities: Targeting

- Computers are used to hold targeting information packages (TIP)
  - Ramzi Yousef 1993 WTC bombing
  - Information found on water systems
  - CAD information on dams found
  - SCADA evidence that al Qaeda operators spent time on sites that offer software and programming instructions for the digital switches that run power, water, transport and communications grids

washingtonpost.com

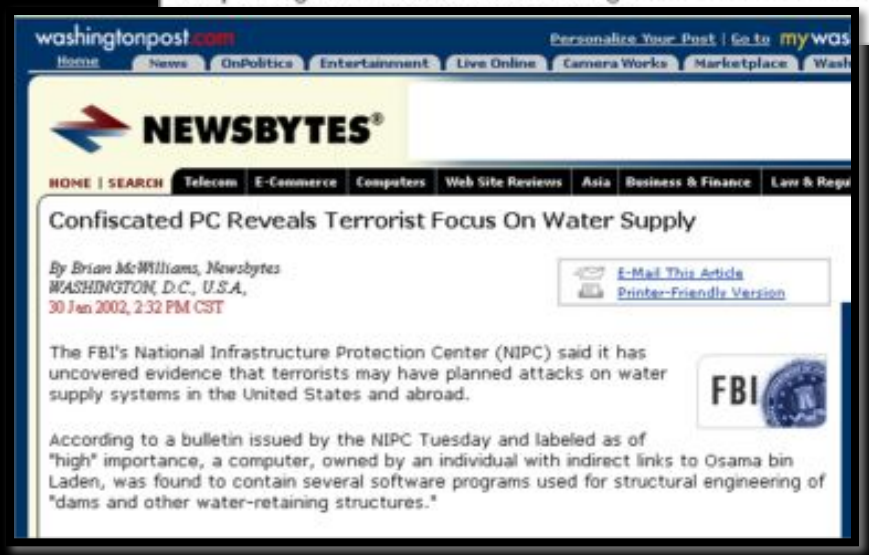
Cyber-Attacks by Al Qaeda Feared

Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say

By Barton Gellman
Washington Post Staff Writer
Thursday, June 27, 2002; Page A01

Late last fall, Detective Chris Hsiung of the Mountain View, Calif., police department
browsers were exploring the digital systems used to manage Bay Area utilities and g

Working with experts at the Lawrence Livermore National Laboratory, the FBI trac
"multiple casings of sites" nationwide. Routed through telecommunications switches i



washingtonpost.com

Home | News | OnPolitics | Entertainment | Live Online | Camera Works | Marketplace

NEWSBYTES®

HOME | SEARCH | Telecom | E-Commerce | Computers | Web Site Reviews | Asia | Business & Finance

Confiscated PC Reveals Terrorist Focus On Water Supply

By Brian McWilliams, Newsbytes
WASHINGTON, D.C., U.S.A.,
30 Jan 2002, 2:32 PM CST

E-Mail This Article
Printer-Friendly Version

The FBI's National Infrastructure Protection Center (NIPC) said it has uncovered evidence that terrorists may have planned attacks on water supply systems in the United States and abroad.

FBI

According to a bulletin issued by the NIPC Tuesday and labeled as of "high" importance, a computer, owned by an individual with indirect links to Osama bin Laden, was found to contain several software programs used for structural engineering of "dams and other water-retaining structures."

Targeting: Analysis

- Terrorist organizations are using information technologies to:
  - Gather targeting information
  - Create targeting information packages
- There are some indications that cyber attacks may come in the future

Unconventional Warfare

- Osama bin Laden
  - "hundreds of young men had pledged to him that they were ready to die and that hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and (sic) ranging from computers to electronics against the infidels."
- Mapping US vulnerabilities

COMPUTER WEEK | GOVERNMENT E-BUSINESS | TECHNOLOGY | EVENTS | LINKS |

Federal Computer Week

Al Qaeda cyber alarm sounded

BY William Matthews
July 25, 2002

Printing? Use this version.
Email this to a friend.

There is a 50 percent chance that the next time al Qaeda terrorists strike the United States, their attack will include a cyberattack, Rep. Lamar Smith (R-Texas) warned.

In closed-door briefings for members of Congress, Smith said officials from federal law enforcement and intelligence-gathering agencies disclosed that al Qaeda operatives have been exploring U.S. Web sites and probing the electronic

RELATED LINKS

"Infosec research bill amended" [FCW.com, May 21, 2002]

"GAO: Fed cyber center falls short" [Federal Computer Week, May 28, 2001]

"Industry hails cyber R&D

Unconventional Warfare

Central Intelligence Agency 2002

- Possibility of cyber warfare attack by terrorists
- Target: Critical infrastructure systems
- Terrorist groups including al-Qa'ida and Hizballah becoming more adept at using the Internet and computer technologies
- Groups most likely to conduct such operations include al-Qa'ida and the Sunni extremists

Compound Attacks

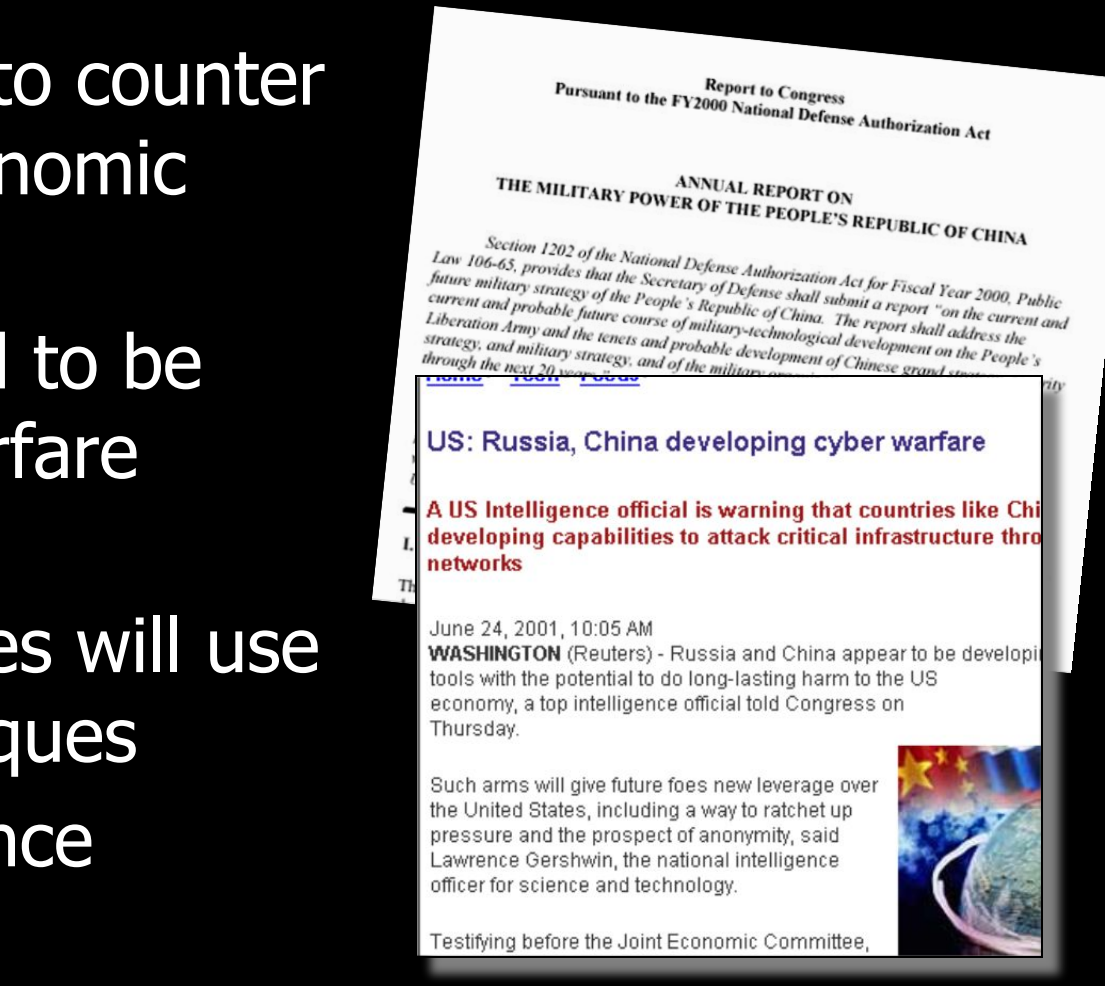
- Employ some or all of aforementioned cyber attacks
- Possibly combined with conventional (physical) terror attack
- Consequences include devastating disruption in communication and commerce

Unconventional Warfare: Analysis

- Both the terrorist groups and government sources indicate that cyber attacks are coming
- Technically advanced operatives are recruited
- Technologies are broadly available
- Vulnerabilities are known
- Compound / blended attacks likely

Nation States

- Asymmetric warfare to counter U.S. military and economic superiority
- 20-30 states believed to be developing cyber warfare capabilities
- Targeted nation-states will use cyber warfare techniques
- Professional intelligence services



Report to Congress
Pursuant to the FY2000 National Defense Authorization Act

ANNUAL REPORT ON
THE MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA

Section 1202 of the National Defense Authorization Act for Fiscal Year 2000, Public Law 106-65, provides that the Secretary of Defense shall submit a report "on the current and future military strategy of the People's Republic of China. The report shall address the current and probable future course of military-technological development on the People's Liberation Army and the tenets and probable development of Chinese grand strategy, and military strategy, and of the military

US: Russia, China developing cyber warfare

A US Intelligence official is warning that countries like Chi developing capabilities to attack critical infrastructure thro networks

June 24, 2001, 10:05 AM
WASHINGTON (Reuters) - Russia and China appear to be developi tools with the potential to do long-lasting harm to the US economy, a top intelligence official told Congress on Thursday.

Such arms will give future foes new leverage over the United States, including a way to ratchet up pressure and the prospect of anonymity, said Lawrence Gershwin, the national intelligence officer for science and technology.

Testifying before the Joint Economic Committee,

Conclusions

- Political conflicts accompanied by cyber attacks
- Cyber attacks escalating in volume, sophistication and coordination
- 'Nuisance attacks' will continue
- Targeted cyber attacks possible
  - (most likely in combination with conventional terrorism compound attack)
- Defense mechanism: international communications, increased vigilance, and continued research and development of security measures

Cyber Reconnaissance

- **Active Reconnaissance**
- **Passive Reconnaissance**
- **Methods**
  - **Port Scanning**
    - **Port scanning methods (**TCP Null, TCP SYN, TCP Xmas, TCP FIN and UDP port scan)
  - **OS Fingerprinting**

OS Fingerprinting

- is a method for determining which operating system does the remote computer runs
- port scanning method to successfully fingerprint the operating system.
- These method can be examining default TCP window size in a packet, measuring data in ICMP packets, guessing TCP initial sequence number etc.
- TCP Banner- Namp and Ring are the tool widely used for OS fingerprinting.

Crimes in Cyber Space-Global Trends & classification

- The volume, scope and cost of cybercrime have reached very high levels
- Crime-as-a-Service
- Ransomware
- The criminal use of data
- Payment fraud
- Online child sexual abuse
- Social engineering
- Virtual currencies

e-commerce security

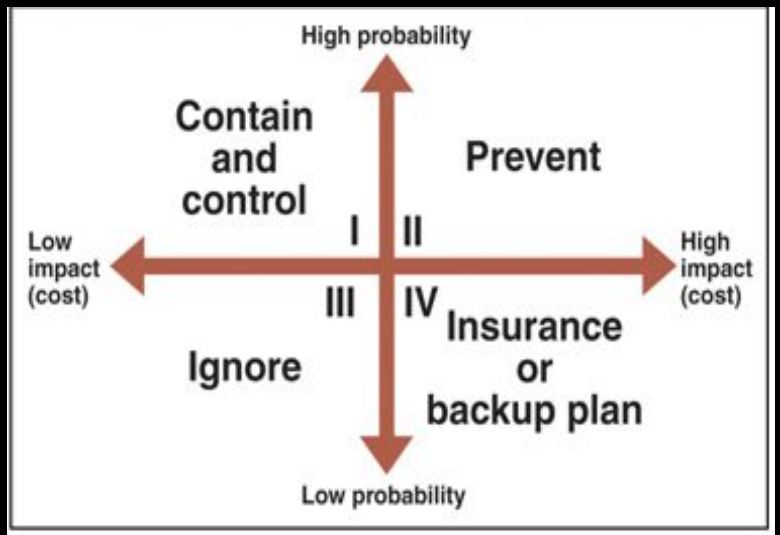
Online Security Issues Overview

- Computer security
  - The protection of assets from unauthorized access, use, alteration, or destruction
- Physical security
  - Includes tangible protection devices
- Logical security
  - Protection of assets using nonphysical means
- Threat
  - Any act or object that poses a danger to computer assets

Managing Risk

Terms --

- Countermeasure
  - General name for a procedure that recognizes, reduces, or eliminates a threat
- Eavesdropper
  - Person or device that can listen in on and copy Internet transmissions
- Crackers or hackers
  - Write programs or manipulate technologies to obtain unauthorized access to computers and networks



Computer Security Classification

- Secrecy/Confidentiality
  - Protecting against unauthorized data disclosure
  - Technical issues
- Privacy
  - The ability to ensure the use of information about oneself
  - Legal Issues
- Integrity
  - Preventing unauthorized data modification by an unauthorized party
- Necessity
  - Preventing data delays or denials (removal)
- Nonrepudiation
  - Ensure that e-commerce participants do not deny (i.e., repudiate) their online actions
- Authenticity
  - The ability to identify the identity of a person or entity with whom you are dealing on the Internet

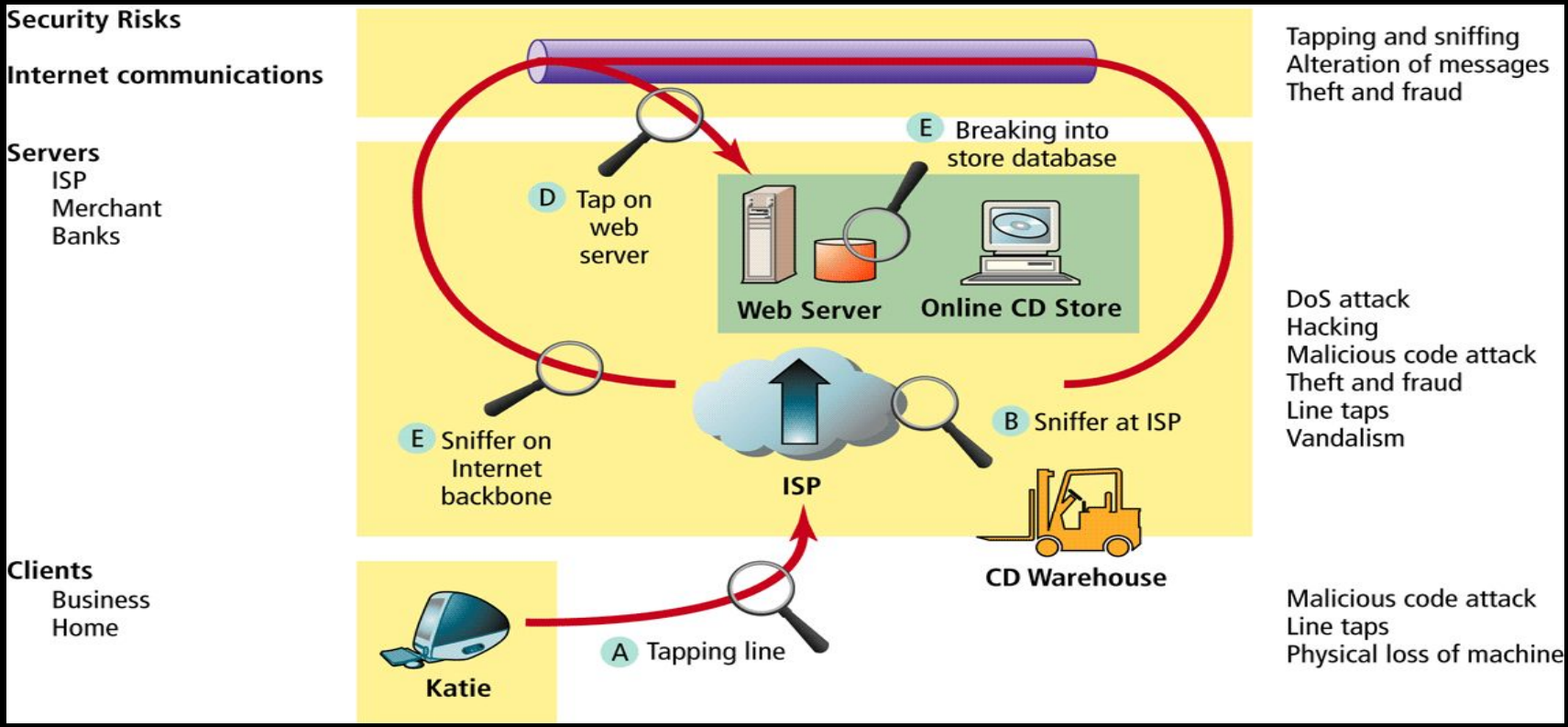
Some solutions --

Requirement	Meaning
Secrecy	Prevent unauthorized persons from reading messages and business plans, obtaining credit card numbers, or deriving other confidential information.
Integrity	Enclose information in a digital envelope so that the computer can automatically detect messages that have been altered in transit.
Availability	Provide delivery assurance for each message segment so that messages or message segments cannot be lost undetectably.
Key management	Provide secure distribution and management of keys needed to provide secure communications.
Nonrepudiation	Provide undeniable, end-to-end proof of each message's origin and recipient.
Authentication	Securely identify clients and servers with digital signatures and certificates.

Security Threats in the E-commerce Environment

Three key points of vulnerability

- the client
- communications pipeline
- the server



Active Content

- Active content refers to programs embedded transparently in Web pages that cause an action to occur
- Scripting languages
  - Provide scripts, or commands, that are executed
- Applet
  - Small application program
  - Java
  - Active X
- Trojan horse
  - Program hidden inside another program or Web page that masks its true purpose
- Zombie
  - Program that secretly takes over another computer to launch attacks on other computers
  - Attacks can be very difficult to trace to their creators

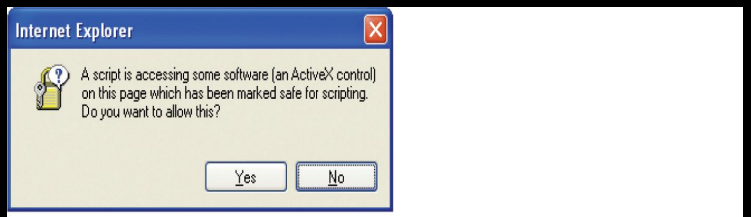


FIGURE 10-5 Dialog box asking for permission to open active content on a Web page

Digital Certificates

- A digital certificate is a program embedded in a Web page that verifies that the sender or Web site is who or what it claims to be
- A certificate is signed code or messages that provide proof that the holder is the person identified by the certificate
- Certification authority (CA)

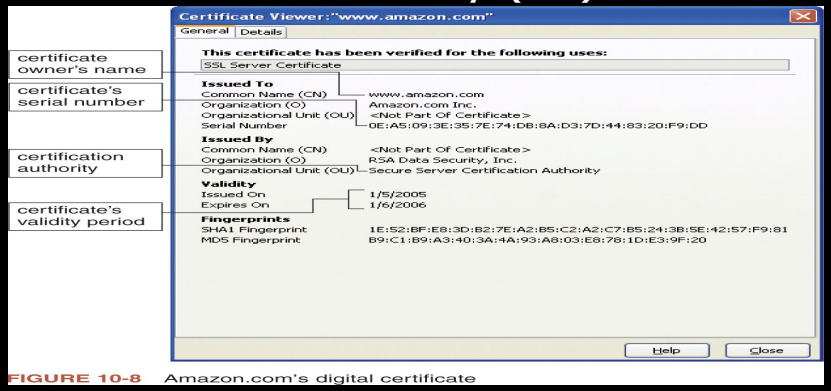


FIGURE 10-8 Amazon.com's digital certificate

- Main elements:
  - Certificate owner's identifying information
  - Certificate owner's public key
  - Dates between which the certificate is valid
  - Serial number of the certificate
  - Name of the certificate issuer
  - Digital signature of the certificate issuer

Communication Channel Security

- Recall that --
  - Secrecy is the prevention of unauthorized information disclosure
  - Privacy is the protection of individual rights to nondisclosure
- Sniffer programs
  - Provide the means to record information passing through a computer or router that is handling Internet traffic

Other Threats

Integrity

- Integrity threats exist when an unauthorized party can alter a message stream of information
- Cybervandalism
  - Electronic defacing of an existing Web site's page
- Masquerading or spoofing
  - Pretending to be someone you are not
- Domain name servers (DNSs)
  - Computers on the Internet that maintain directories that link domain names to IP addresses

Anonymizer

A Web site that provides a measure of secrecy as long as it's used as the portal to the Internet
http://www.anonymizer.com

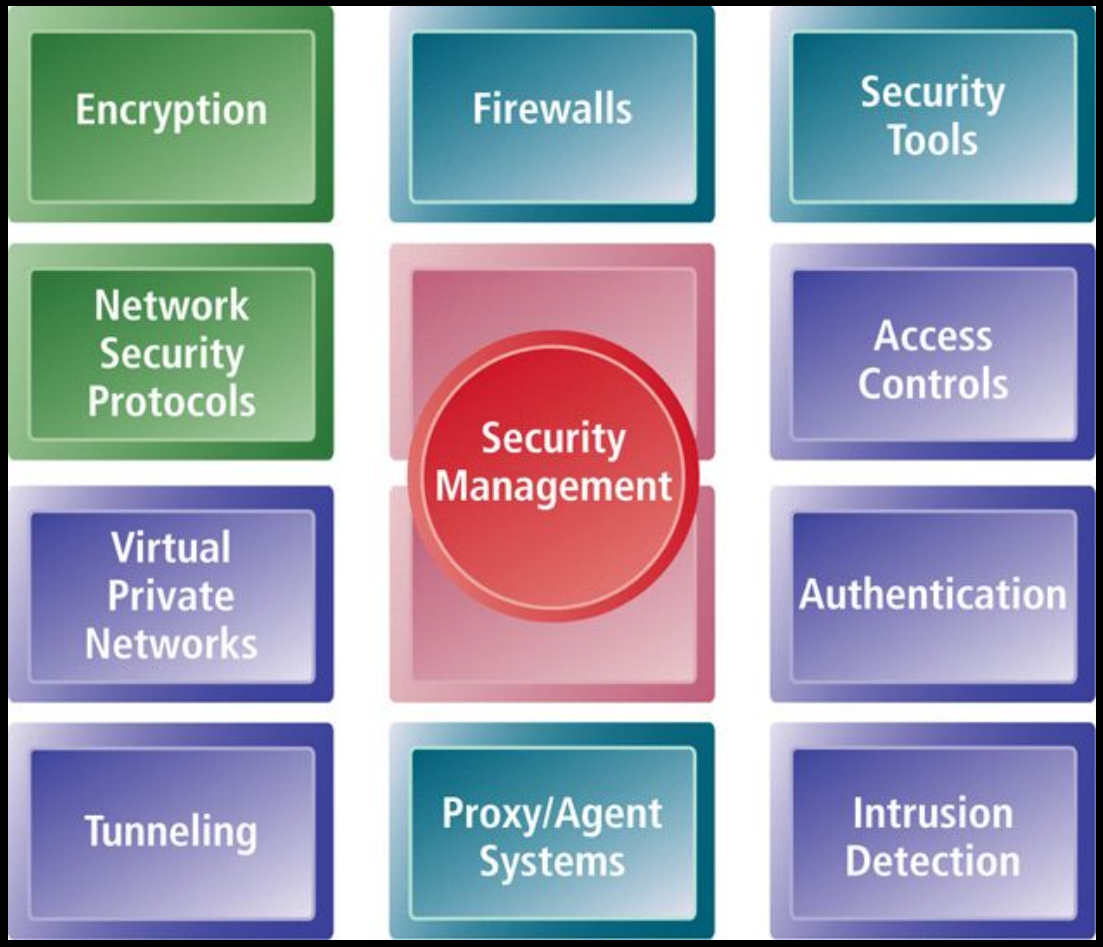
Necessity

- Purpose is to disrupt or deny normal computer processing
- DoS attacks
  - Remove information altogether
  - Delete information from a transmission or file

Wireless Network Threats

- Wardrivers
  - Attackers drive around using their wireless-equipped laptop computers to search for accessible networks
- Warchalking
  - When wardrivers find an open network they sometimes place a chalk mark on the building

Tools Available to Achieve Site Security



Computer Forensics

Introduction

- Topics to be covered
  - Defining Computer Forensics
  - Reasons for gathering evidence
  - Who uses Computer Forensics
  - Steps of Computer Forensics
  - Handling Evidence
  - Investigation initiation / response
  - Handling Information
  - Requirements
  - Anti-Forensics
  - Evidence processing guidelines
  - Methods of hiding Information/data
  - Methods of discovering information/data

Definition

- What is Computer Forensics??
  - Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.
  - Evidence might be required for a wide range of computer crimes and misuses
  - Multiple methods of
    - Discovering data on computer system
    - Recovering deleted, encrypted, or damaged file information
    - Monitoring live activity
    - Detecting violations of corporate policy
  - Information collected assists in arrests, prosecution, termination of employment, and preventing future illegal activity

Definition (cont)

- What Constitutes Digital Evidence?
  - Any information being subject to human intervention or not, that can be extracted from a computer.
  - Must be in human-readable format or capable of being interpreted by a person with expertise in the subject.
- Computer Forensics Examples
  - Recovering thousands of deleted emails
  - Performing investigation post employment termination
  - Recovering evidence post formatting hard drive
  - Performing investigation after multiple users had taken over the system

Reasons For Evidence

- Wide range of computer crimes and misuses
  - Non-Business Environment: evidence collected by Federal, State and local authorities for crimes relating to:
    - Theft of trade secrets
    - Fraud
    - Extortion
    - Industrial espionage
    - Position of pornography
    - SPAM investigations
    - Virus/Trojan distribution
    - Homicide investigations
    - Intellectual property breaches
    - Unauthorized use of personal information
    - Forgery
    - Perjury

Reasons For Evidence (cont)

- Computer related crime and violations include a range of activities including:
  - Business Environment:
    - Theft of or destruction of intellectual property
    - Unauthorized activity
    - Tracking internet browsing habits
    - Reconstructing Events
    - Inferring intentions
    - Selling company bandwidth
    - Wrongful dismissal claims
    - Sexual harassment
    - Software Piracy

Who Uses Computer Forensics?

- Criminal Prosecutors
  - Rely on evidence obtained from a computer to prosecute suspects and use as evidence
- Civil Litigations
  - Personal and business data discovered on a computer can be used in fraud, divorce, harassment, or discrimination cases
- Insurance Companies
  - Evidence discovered on computer can be used to mollify costs (fraud, worker's compensation, arson, etc)
- Private Corporations
  - Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases

Steps Of Computer Forensics

- According to many professionals, Computer Forensics is a four (4) step process
  - Acquisition
    - Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices
  - Identification
    - This step involves identifying what data could be recovered and electronically retrieving it by running various Computer Forensic tools and software suites
  - Evaluation
    - Evaluating the information/data recovered to determine if and how it could be used again the suspect for employment termination or prosecution in court

Steps Of Computer Forensics (cont)

- Presentation
  - This step involves the presentation of evidence discovered in a manner which is understood by lawyers, non-technically staff/management, and suitable as evidence as determined by United States and internal laws

Computer Forensic Requirements

- Hardware
  - Familiarity with all internal and external devices/components of a computer
  - Thorough understanding of hard drives and settings
  - Understanding motherboards and the various chipsets used
  - Power connections
  - Memory
- BIOS
  - Understanding how the BIOS works
  - Familiarity with the various settings and limitations of the BIOS

Computer Forensic Requirements
(cont)

- Operation Systems
  - Windows 3.1/95/98/ME/NT/2000/2003/XP
  - DOS
  - UNIX
  - LINUX
  - VAX/VMS
- Software
  - Familiarity with most popular software packages such as Office
- Forensic Tools
  - Familiarity with computer forensic techniques and the software packages that could be used

Anti-Forensics

- Software that limits and/or corrupts evidence that could be collected by an investigator
- Performs data hiding and distortion
- Exploits limitations of known and used forensic tools
- Works both on Windows and LINUX based systems
- In place prior to or post system acquisition

Evidence Processing Guidelines

- New Technologies Inc. recommends following 16 steps in processing evidence
- They offer training on properly handling each step
  - Step 1: Shut down the computer
    - Considerations must be given to volatile information
    - Prevents remote access to machine and destruction of evidence (manual or ant-forensic software)
  - Step 2: Document the Hardware Configuration of The System
    - Note everything about the computer configuration prior to re-locating

Evidence Processing Guidelines (cont)

- Step 3: Transport the Computer System to A Secure Location
  - Do not leave the computer unattended unless it is locked in a secure location
- Step 4: Make Bit Stream Backups of Hard Disks and Floppy Disks
- Step 5: Mathematically Authenticate Data on All Storage Devices
  - Must be able to prove that you did not alter any of the evidence after the computer came into your possession
- Step 6: Document the System Date and Time
- Step 7: Make a List of Key Search Words
- Step 8: Evaluate the Windows Swap File

Evidence Processing Guidelines (cont)

- Step 9: Evaluate File Slack
  - File slack is a data storage area of which most computer users are unaware; a source of significant security leakage.
- Step 10: Evaluate Unallocated Space (Erased Files)
- Step 11: Search Files, File Slack and Unallocated Space for Key Words
- Step 12: Document File Names, Dates and Times
- Step 13: Identify File, Program and Storage Anomalies
- Step 14: Evaluate Program Functionality
- Step 15: Document Your Findings
- Step 16: Retain Copies of Software Used

Methods Of Hiding Data

- Covert Channels – Hiding in Transmission
  - Take advantage of timing or shared storage to pass data through unsuspected channel

- EXAMPLE: IP datagram – Header Redundancy
  - Known Maximum Transfer Unit (MTU)
    - A datagram (IP) is encapsulated into frame (header, datagram, trailer). MTU is the max total size of this datagram.
    - To make IP independent of physical network, MTU = 65,535 bytes to give it more efficiency.
    - If the physical layer doesn't support that MTU, the datagram must be fragmented

Methods Of Hiding Data (cont)

- EXAMPLE: Continued…
  - Flags: 3 bits
    - 1st bit: reserved (always 0)
    - 2nd bit: Do not fragment (DF): if 1, can't be fragmented. If it is too large to pass through any available physical network, it is discarded
    - 3rd bit: More fragment (MF): if 1, the datagram is not the last fragment of the original datagram, if 0, it is last one or there is only 1 fragment (the original datagram)

Methods Of Hiding Data (cont)

- EXAMPLE – TCP/IP Continued…
  - An un-fragmented datagram has all 0's in the flag fields
    - Redundancy condition: the DF bit can be 1 or 0 if no fragment
    - From network perspective: Datagram 1 is not allowed to fragment (1 bit), datagram 2 is allowed but does not because it is under the maximum MTU size.

Datagram 1	16-bit Id. field	3-bit flag field	13-bit frag. offset	16-bit Total len.
1	XX…XX	0 **1** 0	00...00	472

Datagram 2	16-bit Id. field	3-bit flag field	13-bit frag. offset	16-bit Total len.
1	XX…XX	0 **0** 0	00...00	472

Methods Of Hiding Data (cont)

- To human eyes, data usually contains known forms, like images, e-mail, sounds, and text. Most Internet data naturally includes gratuitous headers, too. These are media exploited using new controversial logical encodings: steganography and marking.
- **Steganography**: The art of storing information in such a way that the existence of the information is hidden.

Methods Of Hiding Data (cont)

- **T**o **h**uman **e**yes, **d**ata **u**sually **c**ontains **k**nown **f**orms, **l**ike **i**mages, **e**-mail, **s**ounds, **a**nd **t**ext. **M**ost **I**nternet **d**ata **n**aturally **i**ncludes **g**ratuitous **h**eaders, **t**oo**. T**hese **a**re **m**edia **e**xploited **u**sing **n**ew **c**ontroversial **l**ogical **e**ncodings: **s**teganography **a**nd **m**arking.

- ***The duck flies at midnight. Tame uncle Sam***
  - Simple but effective when done well

Methods Of Hiding Data (cont)

- **Watermarking**: Hiding data within data
  - Information can be hidden in almost any file format.
  - File formats with more room for compression are best
    - Image files (JPEG, GIF)
    - Sound files (MP3, WAV)
    - Video files (MPG, AVI)
  - The hidden information *may* be encrypted, but not necessarily
  - Numerous software applications will do this for you: Many are freely available online

Methods Of Hiding Data (cont)

- Hard Drive/File System manipulation
  - Slack Space is the space between the logical end and the physical end of file and is called the file slack. The logical end of a file comes before the physical end of the cluster in which it is stored. The remaining bytes in the cluster are remnants of previous files or directories stored in that cluster.
    - Slack space can be accessed and written to directly using a hex editor.
    - This does not add any "used space" information to the drive
  - Partition waste space is the rest of the unused track which the boot sector is stored on – usually 10s, possibly 100s of sectors skipped
    - After the boot sector, the rest of the track is left empty

Methods Of Hiding Data (cont)

- Hard Drive/File System manipulation cont…
  - Hidden drive space is non-partitioned space in-between partitions
    - The File Allocation Table (FAT) is modified to remove any reference to the non-partitioned space
    - The address of the sectors must be known in order to read/write information to them
  - Bad sectors occur when the OS attempts to read info from a sector unsuccessfully. After a (specified) # of unsuccessful tries, it copies (if possible) the information to another sector and marks (flags) the sector as bad so it is not read from/written to again
    - users can control the flagging of bad sectors
    - Flagged sectors can be read to /written from with direct reads and writes using a hex editor

Methods Of Hiding Data (cont)

- Hard Drive/File System manipulation cont…
  - Extra Tracks: most hard disks have more than the rated # of tracks to make up for flaws in manufacturing (to keep from being thrown away because failure to meet minimum #).
    - Usually not required or used, but with direct (hex editor) reads and writes, they can be used to hide/read data
  - Change file names and extensions – i.e. rename a .doc file to a .dll file

Methods Of Hiding Data (cont)

- Other Methods
  - Manipulating HTTP requests by changing (unconstrained) order of elements
    - The order of elements can be preset as a 1 or 0 bit
    - No public software is available for use yet, but the government uses this method for its agents who wish to transfer sensitive information online
    - Undetectable because there is no standard for the order of elements and it is, in essence, just normal web browsing
  - Encryption: The problem with this is that existence of data is not hidden, instead it draws attention to itself.
    - With strong enough encryption, it doesn't matter if its existence is known

Methods Of Detecting/Recovering Data

- Steganalysis - the art of detecting and decoding hidden data
  - Hiding information within electronic media requires alterations of the media properties that may introduce some form of degradation or unusual characteristics
  - The pattern of degradation or the unusual characteristic of a specific type of steganography method is called a signature
  - Steganalysis software can be trained to look for a signature

Methods Of Detecting/Recovering Data (cont)

- Steganalysis Methods - Detection
  - Human Observation
    - Opening a text document in a common word processor may show appended spaces and “invisible” characters
    - Images and sound/video clips can be viewed or listened to and distortions may be found
      - Generally, this only occurs if the amount of data hidden inside the media is too large to be successfully hidden within the media (15% rule)
  - Software analysis
    - Even small amounts of processing can filter out echoes and shadow noise within an audio file to search for hidden information
    - If the original media file is available, hash values can easily detect modifications

Methods Of Detecting/Recovering Data (cont)

- Steganalysis Methods – Detection cont...
  - Disk analysis utilities can search the hard drive for hidden tracks/sectors/data
  - RAM slack is the space from the end of the file to the end of the containing sector. Before a sector is written to disk, it is stored in a buffer somewhere in RAM. If the buffer is only partially filled with information before being committed to disk, remnants from the end of the buffer will be written to disk. In this way, information that was never "saved" can be found in RAM slack on disk.
  - Firewall/Routing filters can be applied to search for hidden or invalid data in IP datagram headers

Methods Of Detecting/Recovering Data (cont)

- Steganalysis Methods – Detection cont...
  - Statistical Analysis
    - Most steganographic algorithms that work on images assume that the Least Significant Bit (LSB) is random
    - If a filter is applied to an image, the LSB bits will produce a recognizable image, so the assumption is wrong
    - After inserting hidden information into an image, the LSB is no longer non-random (especially with encrypted data). If you apply the same filter, it will no longer produce a recognizable image
    - Statistical analysis of the LSB will tell you if the LSB bits are random or not
    - Can be applied to audio files as well (using LSB)
  - Frequency scanning
    - Software can search for high, inaudible frequencies

Methods Of Detecting/Recovering Data (cont)

- Steganalysis Methods – Recovery
  - Recovery of watermarked data is extremely hard
    - Currently, there are very few methods to recover hidden, encrypted data.
  - Data hidden on disk is much easier to find. Once found, if unencrypted, it is already recovered
  - Deleted data can be reconstructed (even on hard drives that have been magnetically wiped)
  - Check swap files for passwords and encryption keys which are stored in the clear (unencrypted)
  - Software Tools
    - Scan for and reconstruct deleted data
    - Break encryption
    - Destroy hidden information (overwrite)

Facebook Forensics

- Due to the popularity of Facebook and its potential for being misused
- Facebook evidences?
- Facebook evidences located?
- How to find out Facebook evidences?

Facebook Protocol Format

- identify the protocol format of Facebook feed, comment, message and chat located in RAM and browser cache on a virtual machine
- **Feed**
  - tester posted a feed “2this is a POST test2” on his own wall
  - replied message “2good to see you POST2”

Feed-HTML format


```
for (;;);{"t":"msg","c":"p_100002239013747","s":3,"ms":[{"updates":["(function(){CSS.show(this);;}).
apply(DOM.find(this.getRelativeTo(),\".uiUfiComments\"))","(function(){DataStore.set(this, \"seqnum\
", \"80230\");}).apply(DOM.find(this.getRelativeTo(),\"\"))","(function(){fc_expand(this, false);}).
apply(DOM.find(this.getRelativeTo(),\"textarea\"))","(function(){(!((DOM.scry(this, \"#optimistic_co
mment_2523124662_0\")).length + (DOM.scry(this, \".comment_80230\")).length)) && DOM.appendContent(D
OM.find(this, \".commentList\"), HTML(\"\\u003cli class=\\\"uiUfiComment comment_80230 ufiItem uiUfi
UnseenItem\\\">\\u003cdiv class=\\\"UIImageBlock clearfix uiUfiActorBlock\\\">\\u003ca class=\\\"act
orPic UIImageBlock_Image UIImageBlock_SMALL_Image\\\" href=\\\"http:\\\/\\\/www.facebook.com\\\/jaso
n.ckyeung\\\" tabindex=\\\"-1\\\">\\u003cimg class=\\\"uiProfilePhoto uiProfilePhotoMedium img\\\" s
rc=\\\"http:\\\/\\\/profile.ak.fbcdn.net\\\/hprofile-ak-snc4\\\/49146_635527479_3483_q.jpg\\\" alt=\
\\\"\\\" \\\/>\\u003c\\\/a>\\u003cdiv class=\\\"commentContent UIImageBlock_Content UIImageBlock_SMAL
L_Content\\\">\\u003ca class=\\\"actorName\\\" href=\\\"http:\\\/\\\/www.facebook.com\\\/jason.ckyeu
ng\\\" data-hovercard=\\\"\\\/ajax\\\/hovercard\\\/user.php?id=635527479\\\">Jason Yeung\\u003c\\\/a
> \\u003cspan data-jsid=\\\"text\\\">\\u200e2good to see you POST2\\u003c\\\/span>\\u003cdiv class=\
\\"commentActions fsm fwn fcg\\\">\\u003cabbr title=\\\"Monday, April 18, 2011 at 4:29pm\\\" data-da
te=\\\"Mon, 18 Apr 2011 01:29:36 -0700\\\" class=\\\"timestamp\\\">2 seconds ago\\u003c\\\/abbr>
```

Feed-JSON format


```
"alert_type":54,"alert_id":505370,"time_created":1303115376,"from_uids":{"635527479":635527479},"fro
m_uid":635527479,"context_id":"108962369188396","total_count":1,"unread":true,"app_id":19675640871,"
oid":"108962369188396","owner":"100002239013747","text":"2good to see you POST2","object_id":"","sto
ry_type":22,"num_credits":0},"userId":"100002239013747","fromId":null,"title":"\u003cspan class=\"bl
ueName\">Jason Yeung\u003c\/span> commented on your status.","body":null,"link":"http:\/\/www.faceboo
k.com\/permalink.php?story_fbid=108962369188396&id=100002239013747"
```

Mobile Device Forensics Overview

Cell Phone Forensics Overview

- Introductions
- Today's Standards and History Of Mobile Device Forensics
- Mobile Forensics is Not Computer Forensics
- Practices and Trends in the Field
- Additional Practices Related To Device Analysis
- Where We're Headed
- Recomendations

Mobile Device Forensics Overview

- Bill Teel
- Working in Mobile Forensics since 2003
- Teel Technologies Established in 2006
- Focus on Mobile Forensic Tools
  Largest Selection in One Place
- Products Include: XRY, Athena, Device Seizure,
  SecureView, Oxygen, Encase, Etc.
- Publisher of MobileForensicsCentral.com
  - Free Search Engine for Mobile Forensics
- Registered Small Business

MOBILE FORENSICS CENTRAL

U.S. Small Business Administration
SBA
Your Small Business Resource

Mobile Device Forensics Overview

Today's Cellular Standards:

Worldwide: +500 Million Subscribers
CDMA is largely in U.S., Asia Pacific (155 Mil), Latin America (71.5 Mil)
source: cdg.org
Major CDMA Network Operators: Verizon, Sprint, Alltel, Leap, U.S. Cellular.

Worldwide: +4.5 Billion Subscribers (including 3G, 4G, WCDMA, HSPDA)
source: gsmworld.com
Major U.S. GSM Network Operators: AT+T, T-Mobile, Alltel, SunCom, Dobson, CellularOne.

– 7 Operators – +30 Million subscribers
Major iDen Operators: Nextel, SouthernLINC Wireless, Boost (MVNO) Telus (Canada)
A Motorola Technology – Only Motorola Phones!

GSM and iDEN Both Use The SIM Card: Subscriber Identity Module

Mobile Device Forensics Overview

Cell Phone Forensics Short History

- **Originated in Europe and focused on the GSM SIM card.** Roaming of Devices from Network and Spectrum Required - I.D. Info on SIM – Also SMS, Phonebooks, and Last Numbers Dialled on SIM
- **Terrorist use of phones as IED detonators** Increased the demand for mobile forensics. Mobile device forensics is making a real impact in the war on terror.
- **Adoption Has Moved Quickly From Federal to Local Level and Now Enterprise, Prisons, Schools, etc.**

Mobile Device Forensics Overview

Mobile Device Forensics Today

Now Used Widely Around the World

- 80% of All Criminal Investigations in Europe Involve Mobile Device Forensics
- 90% of All Criminal Investigations in UK
- 70% in US (estimate and growing)

Quickly Becoming *The Necessary Part* of Every Investigation!

Cell Phone Forensics

First Lesson:

Cell Phone Forensics is NOT Computer Forensics!

While The Intent Is Similar, The Method Is Different

Mobile Device Forensics Overview

The Big Difference:

- **Computer Forensics:** – **Only a Few Major Operating System Standards:** Windows, Mac, Linux. Standard practice is to image the Harddrive and Examine Data.

- **Cell Phone Forensics:** – **Multiple Operating Systems**. Various Communication Standards. Each manufacturer has their own: Nokia, Samsung, Motorola, Palm, Blackberry, etc., etc. Communication Standards Evolving. **Started this way but is consolidating to four or five. Mobile Forensics is becoming more like computer forensics in some ways.**

- **Mobility Aspect:** - **Phones are Live Things Roaming Around**. It's not just about what's on the device, but where has it been and what connections have been made?

Networks Are Managing The Massive Data in Different Ways – Lots There.

What's retained by the network varies from carrier to carrier, but apart from the billing essentials, not much data is saved after 30 days. Some Exceptions.

Mobile Device Forensics Overview

The New York Times

The results were astounding. In a six-month period — from Aug 31, 2009, to Feb. 28, 2010, Deutsche Telekom had recorded and saved his longitude and latitude coordinates more than 35,000 times. It traced him from a train on the way to Erlangen at the start through to that last night, when he was home in Berlin."

http://www.nytimes.com/2011/03/26/business/media/26privacy.html?_r=1

Despite Exceptions - Better to Get Data Sooner Than Later. Location and Data Content Doesn't Typically Does Not Last Long in U.S. – Economics of freeing up storage for networks.

Mobile Device Forensics Overview

Another Difference: Phones Are Always Updating – Proper Handling and Isolation Are Essential

- Cell Phone Forensics is not technically "forensics". We are just starting to image the drive. Mostly we are engaging it to tell us what's in there and then recording and analyzing.

- Proper training in handling and processing phones is essential in reducing the risk of loss or contamination.

- While the acquisition of data is relatively easy, it often requires putting an Agent on the device to assist with data extraction.

- A phone is always updating with the network, and remote destruction is possible. Proper isolation of the device from the network and immediate analysis is best when possible.

Mobile Device Forensics Overview

Another Difference: Phones Are Always Updating – Proper Handling and Isolation Are Essential

- Cell Phone Forensics is not technically "forensics". We are just starting to image the drive. Mostly we are engaging it to tell us what's in there and then recording and analyzing.

- Proper training in handling and processing phones is essential in reducing the risk of loss or contamination.

- While the acquisition of data is relatively easy, it often requires putting an Agent on the device to assist with data extraction.

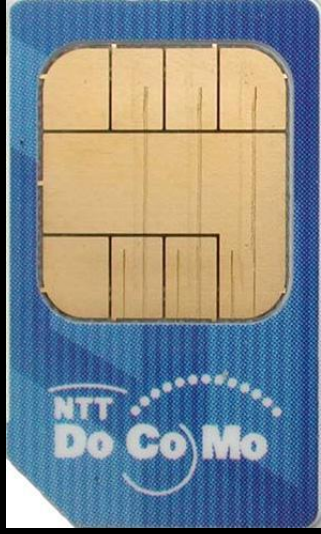
- A phone is always updating with the network, and remote destruction is possible. Proper isolation of the device from the network and immediate analysis is best when possible.

Mobile Device Forensics Overview

What Data is Obtainable?

Mobile Device Forensics Overview

Start with the SIM on GSM Phones



- IMSI: International Mobile Subscriber Identity
- ICCID: Integrated Circuit Card Identification (SIM Serial No.)
- MSISDN: Mobile Station Integrated Services Digital Network (phone number)
- Network Information
- LND: Last Number Dialled (sometimes, not always, depends on the phone)
- ADN: Abbreviated Dialled Numbers (Phonebook)
- SMS: Text Messages, Sent, Received, Deleted, Originating Number, Service Center (also depends on Phone)
- SMS Service Center Info: GPRS Service Center Info:
- Location Information: The GSM channel (BCCH) and Location Area Code (LAC) when phone was used last.

* When SIM Locked – Cannot Be Cracked without Network Operator Assistance.

- IMEI: International Mobile Equipment Identity. - To Find IMEI, Type #*06#. IMEI is on the Device, registers with the network, along with IMSI. IMSI+IMEI+MSISDN the most detailed identity information of user.

Remember… Only GSM and Nextel Phones have SIMs. Not in CDMA (Verizon, Sprint)

A PIN Locked SIM is Not Accessible Without PIN – Requires PUK From Carrier

Mobile Device Forensics Overview

What Can Be Pulled from the Device (Best case scenario from Logical Tools)

- Phonebook
- Call History and Details (To/From)
- Call Durations
- Text Messages with identifiers (sent-to, and originating) Sent, received, deleted messages
- Multimedia Text Messages with identifiers
- Photos and Video (also stored on external flash)
- Sound Files (also stored on external flash)
- Network Information, GPS location
- Phone Info (CDMA Serial Number)
- Emails, memos, calendars, documents, etc. from PDAs.
- Today with Smartphones – GPS Info, Social Networking Data

Mobile Device Forensics Overview

What Can Be Pulled from the Device

From Today's iPhone / iPod / iPad

- Focus Today is Getting Image of iPhone and Analyzing for Data.
- Logical Tools Getting Contacts, Call logs, SMS, MMS, Pics – Much more.
- Facebook Contacts, Skype, YouTube data
- Myspace Username and Passwords
- Location from GPS, Cell Towers and Wi-Fi networks

Mobile Device Forensics Overview

What Can Be Pulled from the Device

From Today's Blackberry

- Most Difficult of Smartphone Devices To Pull Data
- Limited Deleted Data acquired
- A Handset PIN locked Device All But Impossible To Access
- Common practice is to Get IPD "Back-Up" File and Analyze it.
- Call Logs, SMS, Pictures, Phonebook, Email, Location info from IPD Back-up file.

Mobile Device Forensics Overview

What Can Be Pulled from the Device

From Today's Android Device

- Logical Tools Acquiring Call Logs, Pics, Phonebooks
- SIMs on many Androids Providing Last Numbers Dialled and SMS messages
- Physical Access improving. Practioners Rooting Device to Obtain More Data – Parsing Required.
- Most actively pursued device by mobile forensic tool players.

Mobile Device Forensics Overview

Network Call Data Records

Mobile Device Forensics Overview

Beyond the Device - Essential Areas of Mobile Device Forensics Investigations:

Call Data Records

Most Data Relative to What The Network Bills Us For

Mobile Device Forensics Overview

Other Data Available For Investigators
Call Data Records "CDR"

Data Acquired From Call Data Records

- **Number Called and Received**
- **Switch Center / Server Identification (2G/3G Network Interface)**
- **Call Type for Billing Purposes (Day/Night + Weekend)**
- **Length of Call**
- **Start and Stop Time**
- **Location Area Code (LAC)**
- **Cell Identity – Start CI and Finish CI**

Can Also Include:

- **Tower Location Name and GPS Coordinates**
- **Voicemail Call Number**
- **SMS Service Center Number… and more**

Mobile Device Forensics Overview

Sample Call Data Record

Voice Usage For: (203) 855-5387
Account Number: 3040503059

Item	Date	Time	Number Called	Calls To	Mins	Feature Used	Usage Type	Charge	Roam Type	Switch Code	Sid	Serving Area	LAC	Start / End Cl
1	03/14/08	4:32P	(203) 246-0430	NORWALK	5	M2MTMB	DT	$0.00	H	BOTNM0	T-Mobile / Connecticut	Fairfield CT	32199	62681 / 62681
2	03/14/08	4:42P	(203) 556-7836	INCOMING	2	M2MCNG	DT	$0.00	H	BOTNM0	T-Mobile / Connecticut	Fairfield CT	32199	63562 / 63221
3	03/14/08	5:02P	(203) 424-1234	STAMFORD	12	M2MCNG	DT	$0.00	H	BOTNM0	T-Mobile / Connecticut	Fairfield CT	32199	60102 / 60118
4	03/14/08	5:10P	(203) 556-7836	STAMFORD	5	M2MCNG	DT	$0.00	H	BOTNM0	T-Mobile / Connecticut	Fairfield CT	32199	50002 / 50002
5	02/05/08	6:39P	(203) 424-1230	STAMFORD	2	M2MCNG	DT	$0.00	H	BOTNM0	T-Mobile /	Fairfield CT	32199	60103 / 50002

These Are The Basics – Much More Available!
Voicemail, SMS & Data Often Provided Separately

You Only Get What You Ask For!

Mobile Device Forensics Overview

Cell Site Analysis

Mobile Device Forensics Overview

Other Data Available For Investigators - Cell Site Analysis

What Is It?

The Analysis of a Mobile Network's Radio Signal Coverage Relative to Its Users

Mobile Device Forensics Overview

Other Data Available For Investigators - Cell Site Analysis

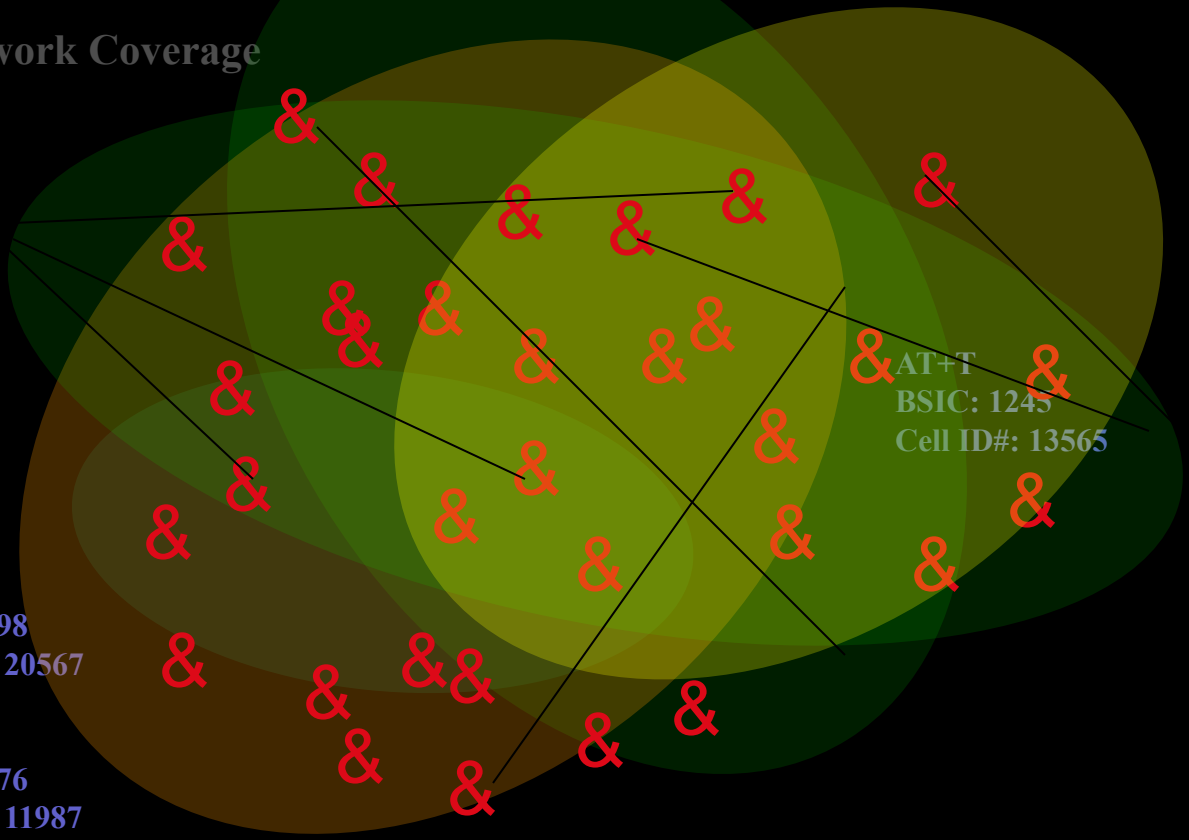
How Is It Useful?

Cell Site Analysis Shows the Real Coverage of the Network's Signal – Used In Conjunction with Network Call Data Records to Prove / Disprove Users Location on the Network.

Gives Examiners the "Real Picture" Of the Network Coverage.

Mobile Device Forensics Overview

Cell Site Analysis



T-Mobile
BSIC: 5498
Cell ID#: 20567

AT+T
BSIC: 9876
Cell ID#: 11987

AT+T
BSIC: 4949
Cell ID#: 20567

T-Mobile
BSIC: 768
Cell ID#: 6776

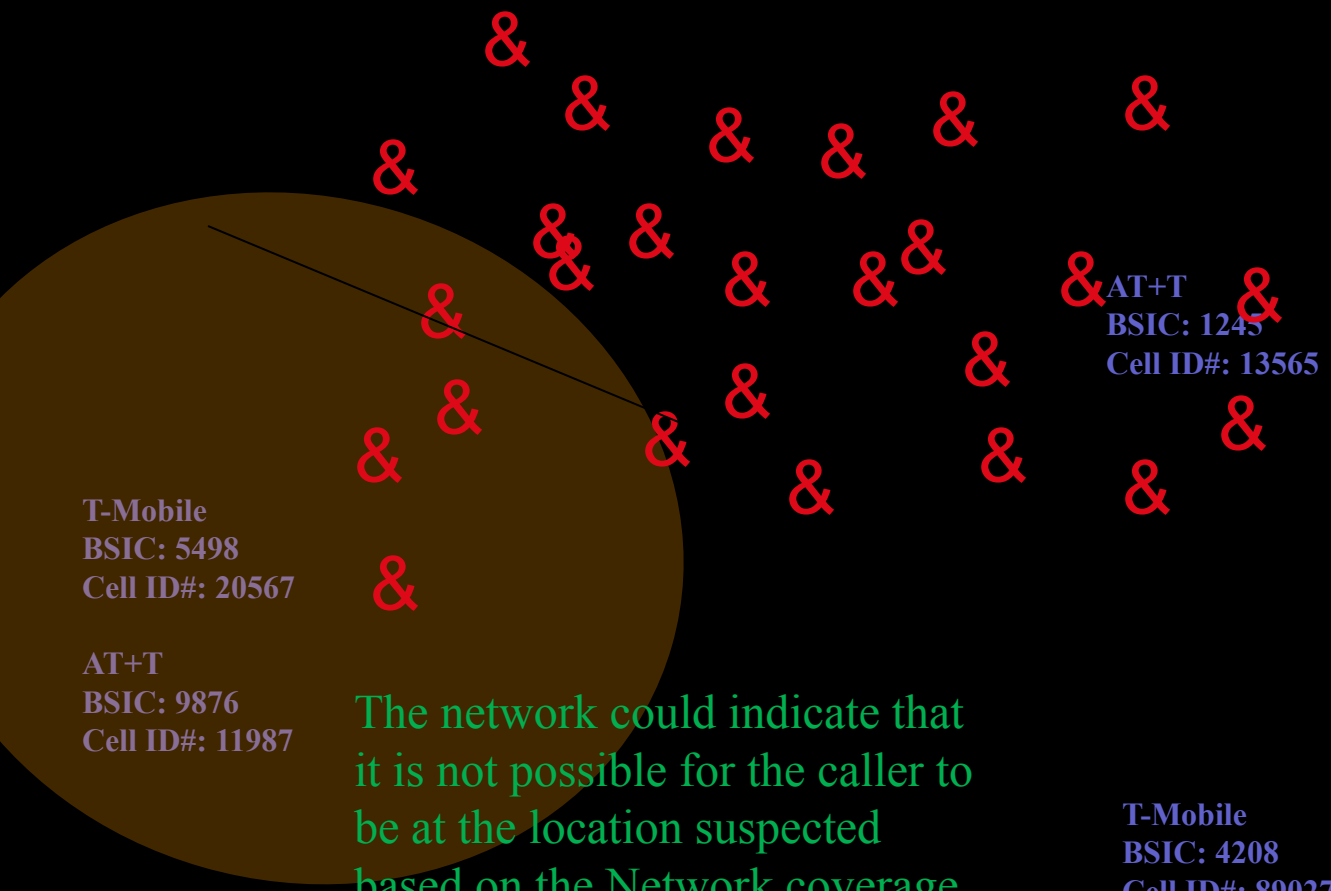
T-Mobile
BSIC: 4208
Cell ID#: 890275

&

Mobile Device Forensics Overview

Cell Site Analysis – What The Network Says…

What The Network Data Would Indicate as to Cell Coverage



AT+T
BSIC: 1245
Cell ID#: 13565

T-Mobile
BSIC: 5498
Cell ID#: 20567

AT+T
BSIC: 9876
Cell ID#: 11987

AT+T
BSIC: 4949
Cell ID#: 20567

T-Mobile
BSIC: 768
Cell ID#: 6776

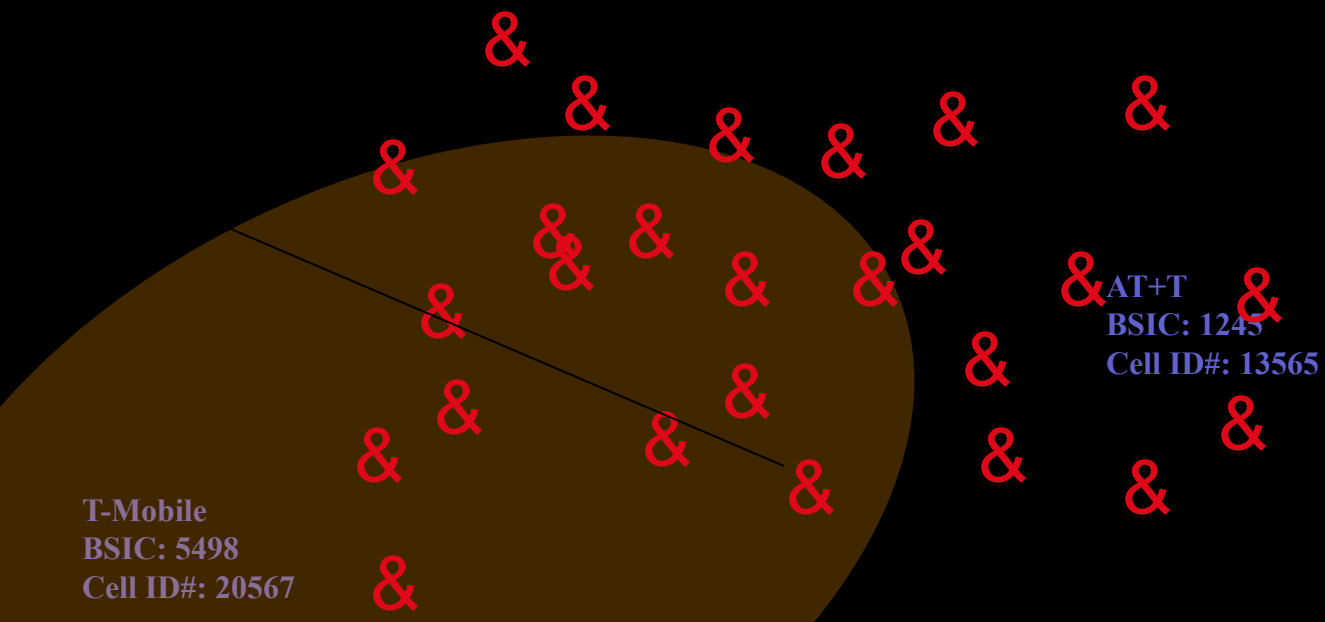
T-Mobile
BSIC: 4208
Cell ID#: 890275

The network could indicate that it is not possible for the caller to be at the location suspected based on the Network coverage data.

Mobile Device Forensics Overview

But The Reality Can Be Far Different.

A Survey of the Network Shows Much Further Coverage.



AT+T
BSIC: 1245
Cell ID#: 13565

T-Mobile
BSIC: 5498
Cell ID#: 20567

AT+T
BSIC: 9876
Cell ID#: 11987

Cell Site Analysis Shows That The Signal Extended To The Location in Question

T-Mobile
BSIC: 4208
Cell ID#: 890275

AT+T
BSIC: 4949
Cell ID#: 20567

T-Mobile
BSIC: 768
Cell ID#: 6776

Mobile Device Forensics Overview

Cell Site Analysis

Cell Identities

Each Base Stations (BTS) on a tower, has its own radio coverage area.

The "Cell" or "Cell Identity" refers to the radio coverage in an area.

Mobile Device Forensics Overview

Surveying The Network As Soon As Possible Provides the Snapshot of Coverage For the Record

AT+T
BSIC: 1245
Cell ID#:
13565

BSIC: 9876
Cell ID#:
11987

BSIC: 4949
Cell ID#:
20567

T-Mobile
BSIC: 4208
Cell ID#:
890275

BSIC: 768
Cell ID#:
6776

BSIC: 5498
Cell ID#:
20567

Logging Network Location Data In Areas of Interest and Cross Referencing with Network Records Allows More Accurate Analysis of User Location on the Network. In Europe, LE is Constantly recording network coverage data to reference with networks when needed.

Mobile Device Forensics Overview

The Femtocell Evolution

Little Towers For The Home

Network Operators are Pushing the Femto (scientific term for something very small) cell to give people an option to use their phones in the home with no charge.

A Wi-Fi like router that connects the caller to their high-speed wireline out of the home.

Benefits for Users: Enables unlimited access and better coverage in the home.

Benefits for Networks: Reduces the traffic on the outer network, offers more services and additional revenue opportunities.

Benefits for Examiners: Provides a record of the user's location when at home. Helps narrow the location of calls.

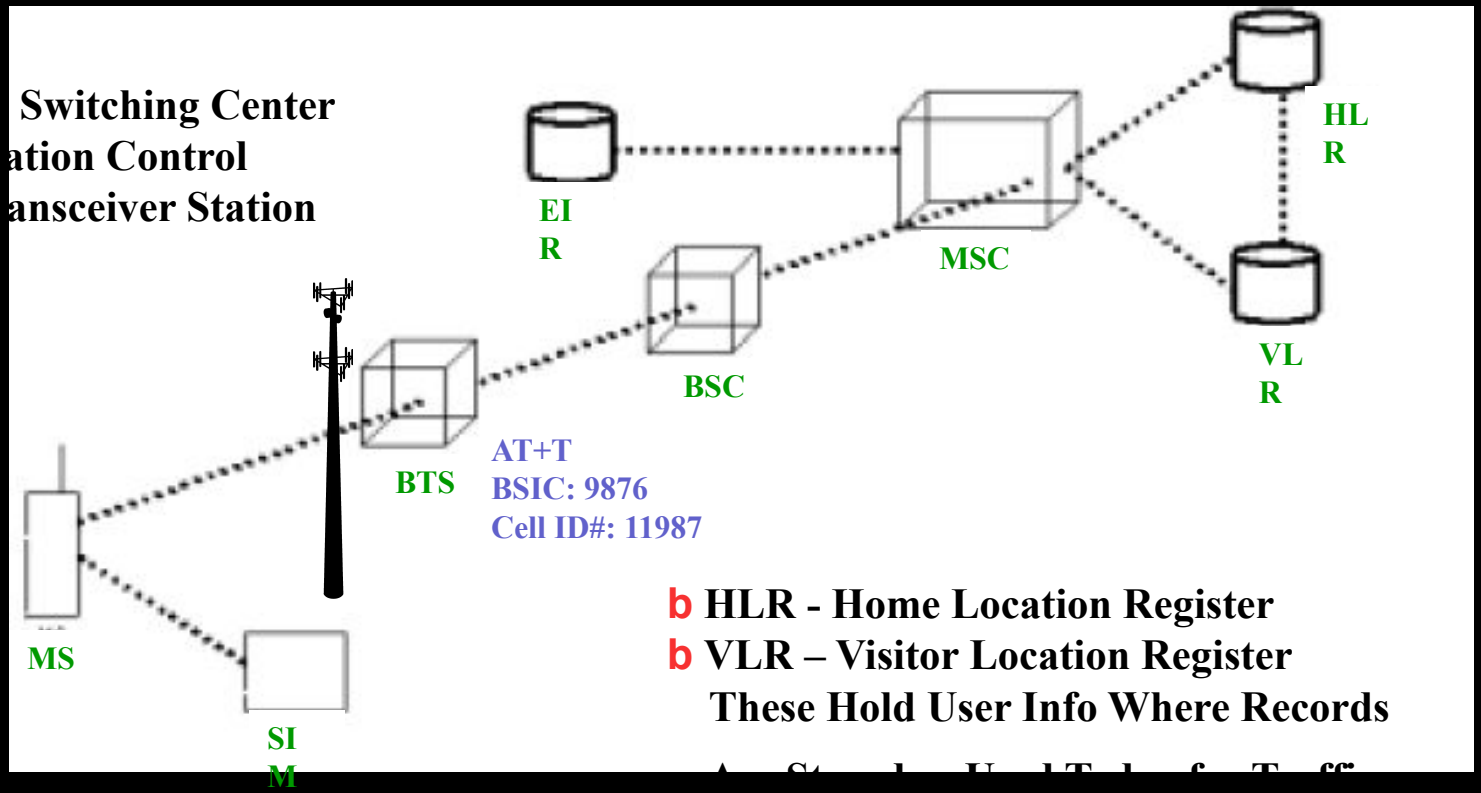
Mobile Device Forensics Overview

The GSM Network in Brief

Network Structure

b

b
b
b



b HLR - Home Location Register
b VLR – Visitor Location Register
These Hold User Info Where Records

Mobile Device Forensics Overview

The Mobile Device Forensic Process
Tools and Techniques of the Trade

Mobile Device Forensics Overview

Data Capture Options

- **Screen Captures:** The simplest way. Use a camera to take pictures of what's on the screen. Reporting tools available. Sometimes this is the only way.

- **Logical Analysis:** – Extracting the data on the device that you see and can access on the device. No deleted information with this method. Call logs, phone books, sms messages, pictures, email, browsing etc. The "active" information on the device can be extracted using a "Logical" extraction tool. This is the standard method today. Plenty of tools and easy to use.

- **Physical Analysis:** – The practice of extracting data from the physical memory of the device, and removable memory. Like PC forensics, you are getting the raw binary / hex data. Requires decoding and understanding of language and techniques used by device manufacturers. Physical analysis is the way to deleted information, but it is difficult and sparsely supported. Only a few tools. Mostly Nokia supported. Early days of the new standard.

- **Chip Level Analysis:** - Analysis of the chips in the phone by removing them from the device and probing for data, or rebuilding another phone

Mobile Device Forensics Overview

Options For Cell Phone Forensics

Chip-Off Analysis

Physical Analysis and Alternative Methods for Extraction

Logical Analysis

Screen Capture and Manual Reporting

Chip-Off Analysis Just Starting to Get Attention.

Most Analysis is Logical Data or Screen Capture.

Mobile Device Forensics Overview

The Unfortunate Reality of Kit…

There Is No One Size Fits All Solution

- A Number of Mobile Device Forensic Tools on the Market
- Each Have Their Strengths and Weaknesses. Plenty of Overlap of Support, but Success with Devices Varies.
- This is due to the challenges in supporting the continuous introductions of new phones and changing technologies. It's a tough job for the examiner to keep up – And equally difficult for the companies making the tools.
- Examiners Never Know What They Are Going To Get! Often need more than one tool for the multiple different devices out there.
- This is changing somewhat with a consolidation of mobile Operating Systems (Android, Apple, BlackBerry, Windows), but it still tools will do or dig deeper in some areas than others.

Cyber Forensics

- Includes:
  - Networks (Network Forensics)
  - Small Scale Digital Devices
  - Storage Media (Computer forensics)
  - Code Analysis

Cyber Forensics

- The scientific examination and analysis of digital evidence in such a way that the information can be used as evidence in a court of law.

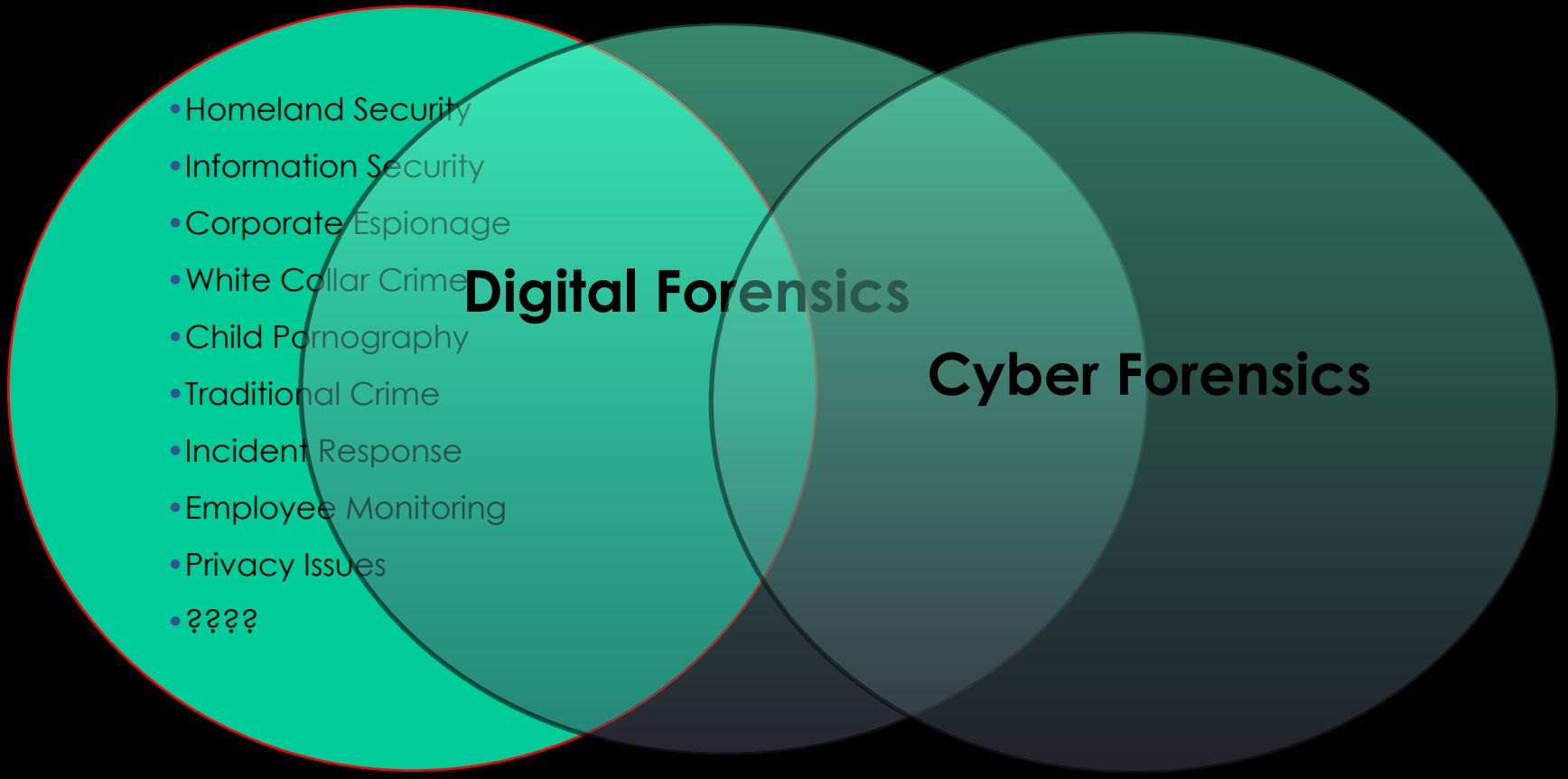
Cyber Forensic Activities

- Cyber forensics activities commonly include:
  - the secure collection of computer data
  - the identification of suspect data
  - the examination of suspect data to determine details such as origin and content
  - the presentation of computer-based information to courts of law
  - the application of a country's laws to computer practice.

The 3 As

- The basic methodology consists of the 3 As:
  - *Acquire* the evidence without altering or damaging the original
  - *Authenticate* the image
  - *Analyze* the data without modifying it

Context of Cyber Forensics



Crime Scenes

- Physical Crime Scenes vs. Cyber/Digital Crime Scenes
- Overlapping principals
- The basics of criminalistics are constant across both physical and cyber/digital
- Locard's Principle applies
  - "When a person commits a crime something is always left at the scene of the crime that was not present when the person arrived"

Digital Crime Scene

- Digital Evidence
  - Digital data that establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and the perpetrator (Carrier & Spafford, 2003)
- Digital Crime Scene
  - The electronic environment where digital evidence can potentially exist (Rogers, 2005)
  - Primary & Secondary Digital Scene(s) as well

Forensic Principles

- Digital/ Electronic evidence is extremely volatile!
- Once the evidence is contaminated it cannot be de-contaminated!
- The courts acceptance is based on the best evidence principle
  - With computer data, printouts or other output readable by sight, and bit stream copies adhere to this principle.
- Chain of Custody is crucial

Cyber Forensic Principles

- **The 6 Principles are:**
  1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
  2. Upon seizing digital evidence, actions taken should not change that evidence.
  3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
  4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
  5. An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.
  6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

Process/Phases

- Identification
- Collection
  - Bag & Tag
- Preservation
- Examination
- Analysis
- Presentation/Report

Identification

- The first step is identifying evidence and potential containers of evidence
- More difficult than it sounds
  - Small scale devices
  - Non-traditional storage media
  - Multiple possible crime scenes

Devices Identification

Identification

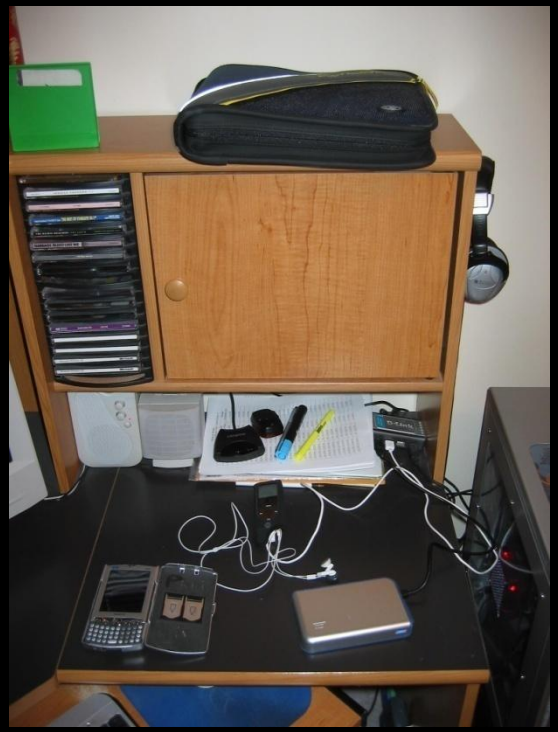
- Context of the investigation is very important
- Do not operate in a vacuum!
- Do not overlook non-electronic sources of evidence
  - Manuals, papers, printouts, etc.

Collection

Care must be taken to minimize contamination

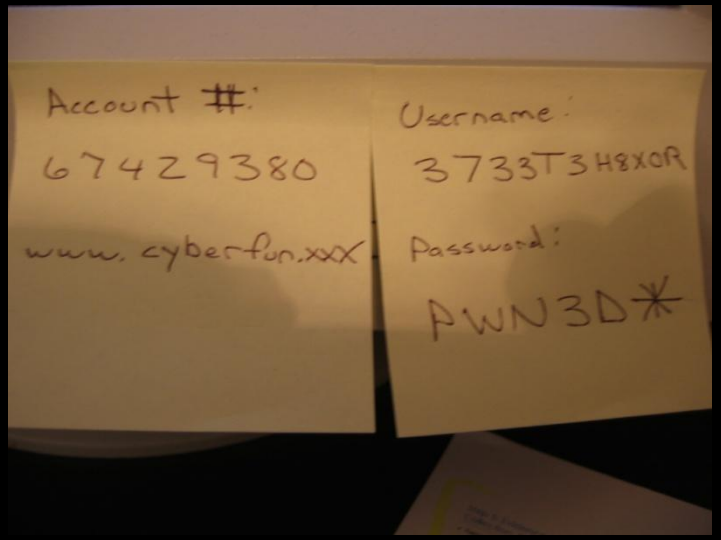
- Collect or seize the system(s)
- Create forensic image
  - Live or Static?
  - Do you own the system
  - What does your policy say?

Collection: Documentation



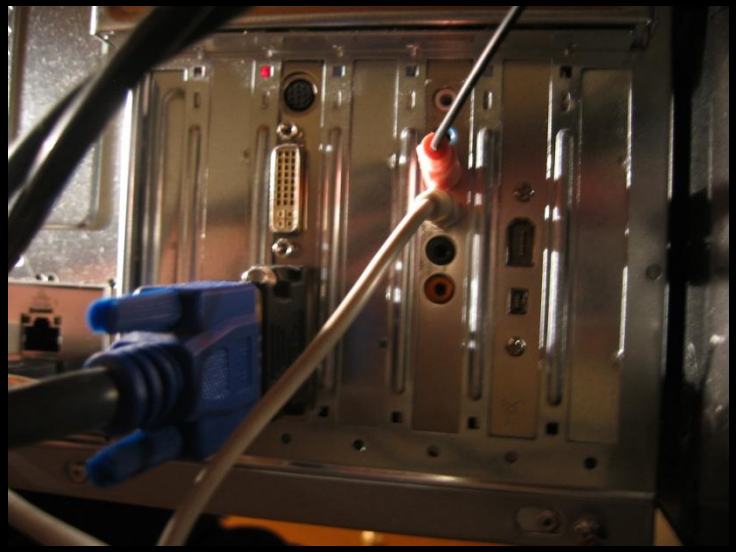
Collection: Documentation

- Take detailed photos and notes of the computer / monitor
  - If the computer is "on", take photos of what is displayed on the monitor – DO NOT ALTER THE SCENE



Collection: Documentation

- Make sure to take photos and notes of all connections to the computer/other devices



Collection: Imaging

- Rule of Thumb: make 2 copies and don't work from the original (if possible)
- A file copy does not recover all data areas of the device for examination
- Working from a duplicate image
  - Preserves the original evidence
  - Prevents inadvertent alteration of original evidence during examination
  - Allows recreation of the duplicate image if necessary

Collection: Imaging

- Digital evidence can be duplicated with no degradation from copy to copy
  - This is not the case with most other forms of evidence

Collection: Imaging

- Write blockers
  - Software
  - Hardware
- Hardware write blockers are becoming the industry standard
  - USB, SATA, IDE, SCSI, SIM, Memory Cards
  - Not BIOS dependent
  - But still verify prior to usage!

Collection: Imaging

- Forensic Copies (Bitstream)
  - Bit for Bit copying captures all the data on the copied media including hidden and residual data (e.g., slack space, swap, residue, unused space, deleted files etc.)
- Often the "smoking gun" is found in the residual data.
- Imaging from a disk (drive) to a file is becoming the norm
  - Multiple cases stored on same media
  - No risk of data leakage from underlying media
- Remember avoid working for original
- Use a write blocker even when examining a copy!

Imaging: Authenticity & Integrity

- How do we demonstrate that the image is a true unaltered copy of the original?

  -Hashing (MD5, SHA 256)

- A mathematical algorithm that produces a unique value (128 Bit, 512 Bit)
  - Can be performed on various types of data (files, partitions, physical drive)
- The value can be used to demonstrate the integrity of your data
  - Changes made to data will result in a different value
- The same process can be used to demonstrate the image has not changed from time-1 to time-n

Examination

- Higher level look at the file system representation of the data on the media
- Verify integrity of image
  - MD5, SHA1 etc.
- Recover deleted files & folders
- Determine keyword list
  - What are you searching for
- Determine time lines
  - What is the timezone setting of the suspect system
  - What time frame is of importance
  - Graphical representation is very useful

Examination

- Examine directory tree
  - What looks out of place
  - Stego tools installed
  - Evidence Scrubbers
- Perform keyword searches
  - Indexed
  - Slack & unallocated space

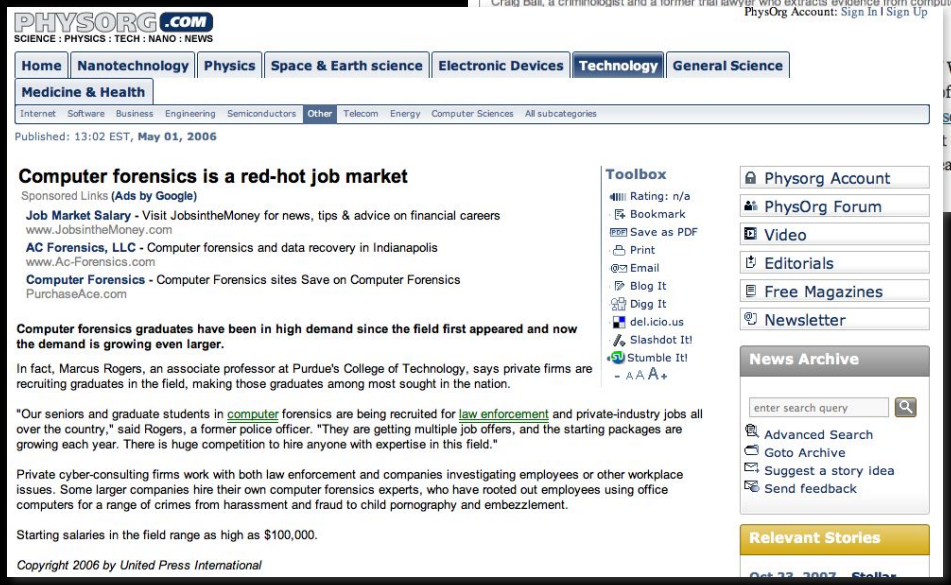
- Search for relevant evidence types
  - Hash sets can be useful
  - Graphics
  - Spreadsheets
  - Hacking tools
  - Etc.
- Look for the obvious first
- When is enough enough??

Issues

- lack of certification for tools
- Lack of standards
- lack of certification for professionals
- lack of understanding by Judiciary
- lack of curriculum accreditation
- Rapid changes in technology!
- Immature Scientific Discipline

Careers

- One of the fastest growing job markets!



Paths to Careers in CF

- Certifications
- Associate Degree
- Bachelor Degree
- Post Grad Certificate
- Masters
- Doctorate

Job Functions

- CF Technician
- CF Investigator
- CF Analyst/Examiner (lab)
- CF Lab Director
- CF Scientist

Professional Opportunities

- Law Enforcement
- Private Sector
- Intelligence Community
- Military
- Academia

Summary

- Cyber Forensics is a maturing forensic Science
- AAFS new section Feb 2008
- Excellent career opportunities
- Proper education & training is paramount!

What is Digital Forensics?

- Emerging discipline in computer security
  - "voodoo science"
  - No standards, few research
- Investigation that takes place after an incident has happened
- Try to answer questions: Who, what, when, where, why, and how

Types of investigations

- Determine what the incident was and get back to a working state
- Internal investigation
  - Should be based on IR policy
  - May lead to criminal investigation
- Criminal investigation
- Support for “real world” investigations

Typical investigation phases

1. Acquisition
2. Recovery
3. Analysis
4. Presentation

Phase 1: Acquisition

- Analogous to crime scene in the "real world"
- Goal is to recover as much evidence without altering the crime scene
- Investigator should document as much as possible
- Maintain *Chain of Custody*

Acquisition (2)

- Determine if incident actually happened
- What kind of system is to be investigated?
  - Can it be shut down?
  - Does it have to keep operating?
- Are there policies governing the handling of the incident?
- Is a warrant needed?

Acquisition (3)

- Get most fleeting information first
  - Running processes
  - Open sockets
  - Memory
  - Storage media
- Create 1:1 copies of evidence (imaging)
- If possible, lock up original system in the evidence locker

Phase 2: Recovery

- Goal is to extract data from the acquired evidence
- Always work on copies, never the original
  - Must be able to repeat entire process from scratch
- Data, deleted data, “hidden” data

File systems

- Get files and directories
- Metadata
  - User IDs
  - Timestamps (MAC times)
  - Permissions, …
- Some deleted files may be recovered
- Slack space

File deletion

- Most file systems only delete directory entries but not the data blocks associated with a file.
- Unless blocks get reallocated the file may be reconstructed
  - The earlier the better the chances
  - Depending on fragmentation, only partial reconstruction may be possible

Slack space

- Unallocated blocks
  - Mark blocks as allocated to fool the file system
- Unused space at end of files if it doesn't end on block boundaries
- Unused space in file system data structures

Steganography

- Data hidden in other data
- Unused or irrelevant locations are used to store information
- Most common in images, but may also be used on executable files, meta data, file system slack space

Encrypted data

- Depending on encryption method, it might be infeasible to get to the information.
- Locating the keys is often a better approach.
- A suspect may be compelled to reveal the keys by law.

Recovery (cont.)

- Locating hidden or encrypted data is difficult and might even be impossible.
- Investigator has to look at other clues:
  - Steganography software
  - Crypto software
  - Command histories

File residue

- Even if a file is completely deleted from the disk, it might still have left a trace:
  - Web cache
  - Temporary directories
  - Data blocks resulting from a move
  - Memory

Phase 3: Analysis

- Methodology differs depending on the objectives of the investigation:
  - Locate contraband material
  - Reconstruct events that took place
  - Determine if a system was compromised
  - Authorship analysis

Contraband material

- Locate specific files
  - Databases of illegal pictures
  - Stolen property
- Determine if existing files are illegal
  - Picture collections
  - Music or movie downloads

Locating material

- Requires specific knowledge of file system and OS.
- Data may be encrypted, hidden, obfuscated
- Obfuscation:
  - Misleading file suffix
  - Misleading file name
  - Unusual location

Event reconstruction

- Utilize system and external information
  - Log files
  - File timestamps
  - Firewall/IDS information
- Establish time line of events

Time issues

- Granularity of time keeping
  - Can’t order events that occur in the same time interval
- Multiple systems:
  - Different clocks
  - Clock drift
- E-mail headers and time zones

The needle in the haystack

- Locating files:
  - Storage capacity approaches the terrabyte magnitude
  - Potentially millions of files to investigate
- Event reconstruction:
  - Dozens, hundreds of events a second
  - Only last MAC times are available
  - Insufficient logging

Compromised system

- If possible, compare against known good state
  - Tripwire
  - Databases of “good” files
- Look for unusual file MACs
- Look for open or listening network connections (trojans)
- Look for files in unusual locations

Unknown executables

- Run them in a constrained environment
  - Dedicated system
  - Sandbox
  - Virtual machine
- Might be necessary to disassemble and decompile
  - May take weeks or months

Authorship analysis

- Determine who or what kind of person created file.
  - Programs (Viruses, Tojans, Sniffers/Loggers)
  - E-mails (Blackmail, Harassment, Information leaks)
- If actual person cannot be determined, just determining the skill level of the author may be important.

Phase 4: Presentation

- An investigator that performed the analysis may have to appear in court as an expert witness.
- For internal investigations, a report or presentation may be required.
- Challenge: present the material in simple terms so that a jury or CEO can understand it.

Forensics Tools

- Acquisition
  - dd, pdd
  - SafeBack, …
- Recovery
  - Encase
  - TCT and SleuthKit
- Analysis
  - ?
- Presentation
  - ?

DF Investigator Profile

- Understanding of relevant laws
- Knowledge of file systems, OS, and applications
  - Where are the logs, what is logged?
  - What are possible obfuscation techniques?
  - What programs and libraries are present on the system and how are they used?
- Know what tools exist and how to use them
- Be able to explain things in simple terms

Future in DF

- The need for standards
  - Acquisition procedure: develop step-by-step instructions to be followed
  - Certification
    - Investigators
    - Tools
    - Operating Systems

Future in DF (2)

- Research
  - Create more meaningful audit data
  - Ensure integrity and availability of audit data
  - Privacy and Digital Forensics
  - Develop detection techniques
  - Develop automation processes

Future in DF (3)

- Documentation
  - File systems
    - Over 50 different FS currently in use
    - Most are poorly documented
  - Malware
    - “fingerprint” of bad programs
  - Good system state
    - Accessible databases
    - Every OS, version, patchlevel