Forensics Technology and Systems

Introduction

Cyber forensics

- Discovery, analysis, and reconstruction of evidence
- Evidence are extracted from
  - computer systems
  - computer networks
  - computer media
  - computer peripherals
- CF focuses on **real-time, online** evidence gathering rather than the traditional offline computer disk forensic technology

Introduction

- Opportunity for cyber crime is increasing
- It is crucial to make advances in
  - Law enforcement
  - Legal
  - Forensic computing technique

Introduction

- Two components of cyber forensics technology
  1. Computer forensics
  2. Network forensics

Introduction

1. **Computer forensics**
   - Deals with gathering evidence from
     - Computer media seized at the crime scene
       - » Involve imaging storage media
       - » Recovering deleted files
       - » Searching slack and free space
     - Preserving the collected information for taking legal action
     - Several computer forensic tools are available to investigators

Introduction

2.Network forensics

- Deals primarily with in-depth analysis of computer network intrusion evidence
- More technically challenging
- 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
- Current commercial intrusion analysis tools are inadequate to deal with today's networked, distributed environments

Introduction

- 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 and support of various objectives,** in addition to traditional postmortem forensic analysis
- This is essential to **continued functioning** of critical information systems and infrastructures
- Only very **few forensic tools** are available to assist in preempting the attacks or locating the perpetrators

Introduction

- Objectives
  - Timely cyber attack containment
  - Perpetrator location and identification
  - Damage mitigation
  - Recovery initiation in the case of a crippled, yet still functioning, network
- Sources of data evidence
  - Intrusion detection system logs
  - Firewall logs
  - Audit trails
  - Network management information
- Also inspect
  - Contents or state of memory
  - Registers
  - Basic input/output system
  - Buffers
  - Cache

Introduction

- Types of computer forensics technology used by
  - Military
  - Law enforcement
  - Business computer specialists

Types of Military Computer Forensic Technology

- Includes **evaluation and indepth examination** of data related to both the **trans- and post-cyberattack**
- Key objectives include
  - **Rapid discovery** of evidence
  - Estimation of **potential impact** of the malicious activity on the victim
  - 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

Types of Military Computer Forensic Technology

- Cyber forensic concepts are new and untested
- National Institute of Justice (NIJ) and National Law Enforcement and Corrections Technology Center (NLECTC) together test new ideas and prototype tools
- The Computer Forensics Experiment 2000 (CFX-2000) resulted from this partnership
- CF technology moved from military research and development (R&D) laboratories into the hands of law enforcement

Types of Military Computer Forensic Technology

- The Computer Forensics Experiment 2000
  - 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

Types of Military Computer Forensic Technology

- CFX-2000
  - CF tools involved are **commercial off-the-shelf software and directorate-sponsored R&D prototypes**
  - The Synthesizing Information from Forensic Investigations (SI-FI) integration environment
    - 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
  - The teams **used other forensic tools and prototypes**
    - to collect and analyze specific features of the 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 Military Computer Forensic Technology

FIGURE 2.1 CFX-2000 schematic

Types of Law Enforcement: Computer Forensic Technology

- CF involves the **preservation, identification, extraction, processing and documentation** of computer evidence
  - Special forensic software tools and techniques are required
    - Tools and techniques
      - Help to hide evidence
      - They are valuable resource for law enforcement
      - Have become important resources for use in internal investigations, civil lawsuits, and computer security risk management
      - Used to create computer evidence without the knowledge of the computer operator

Types of Law Enforcement: Computer Forensic Technology

- Forensic software tools and methods
  - Used to identify passwords, logons, and other information
  - Used to identify backdated files

Types of Law Enforcement: Computer Forensic Technology

- **Computer Evidence Processing Procedures**
  - Processing procedures and methodologies should conform to **federal computer evidence processing standards**
  - Training and certification programs have also been developed for the International Association of Computer Investigation Specialists (IACIS)

Types of Law Enforcement: Computer Forensic Technology

- **Computer Evidence Processing Procedures**
  - Preservation of Evidence
  - Disk Structure
    - evidence can reside at various levels within the structure of the disk
  - Data Encryption
    - should become familiar with different forms
  - Matching a Diskette to a Computer
    - use special software tools to complete this process
  - Data Compression
  - Erased Files
  - Internet Abuse Identification and Detection
  - The Boot Process and Memory Resident Programs

TYPES OF BUSINESS COMPUTER FORENSIC 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

- **Forensic services available**
- 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 monitoringvailable
- 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

Types of Computer Forensics Systems

- **Internet security systems**
- Internet security can provide a more secure solution, as well as onethat 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.

Types of Computer Forensics Systems

- **Internet security systems**

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
- A powerful technique for securely sending information is public key encryption or public key infrastructure.
- Firewalls are a basic means for providing network security.
- Payment gateway secure the payment information provided by the customer to the merchant..
- Variety of security products are available to implement an access control system.
- Secure virtual private networks (SVPN) provide significant reduction in internal corporate networking costs to achieved secure, encrypted, Internet protocol (IP)-level network communications over less expensive public networks.
- Smart card is equivalent to an electronic safe deposit box. A smart card contains a semiconductor chip with logic and nonvolatile memory. The software within the card detects intrusion and tampering and monitors abnormal usage.

Types of Computer Forensics 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.

Types of Computer Forensics Systems

- **Intrusion detection systems**
- 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
- Some systems provide additional features, including
  - Automatic installation of vendor-provided software patches
  - Installation and operation of decoy servers to record information about intruders

Types of Computer Forensics Systems

- **Intrusion detection systems**
  - Vulnerability assessment products (*scanners*) perform rigorous examinations of systems. It provides both passive and active examination to determine weaknesses that might allow security violations.
  -
  - Network security management is a process that establishes and maintains policies, procedures and practices required for protecting networked information system assets.

Types of Computer Forensics Systems

- **Firewall security systems**

- Firewall technology is a first line of defense. It form 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.
- 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
-

Types of Computer Forensics Systems

- **Storage area network security systems**

- Disaster recovery services use storage area networks (SANs). It is used to restore thousands of terabytes of business data and get hundreds of companies running. SANs are a new methodology for attaching storage using a separate network to connects all storage and servers.

- **Network disaster recovery systems**
-
- 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.

Types of Computer Forensics Systems

- **Public key infrastructure systems**
- PKI is an environment that provides trust and confidentiality in data transmission and storage. PKI accomplishes these goals for an enterprise through policy and technology components. Technology component determine and identify the roles, responsibilities, constraints, range of use, and services available.
- 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

Types of Computer Forensics Systems

- **Wireless network security systems**
- Protecting wireless network from viruses is complicated process. Business is working hardly to provide security in wireless network.

- **Satellite encryption security systems**
- Satellite communications is becoming a security nightmare. Providing security is essential to provide protection of intellectual property distribution, electronic commerce, electronic battlefields and national security. Multi layer Encryption on top of compressed data is to be transmitted to a satellite (uplink) from Earth and then transmitted down to Earth (downlink). Then it is decrypted. This compression, multilayer encryption provides confidentiality and authentication.

Types of Computer Forensics Systems

- **Biometric security systems**
- Biometric system is the computer hardware and software used to recognize or verify an individual.

- **Homeland security systems**
- Homeland security is defined as the deterrence, prevention, and preemption of and defense against aggression targeted at a countries territory, sovereignty, population, and infrastructure.
-