COMP 2555 Principles of Computer Forensics

Ramki Thurimella, PhD

Overview

- Review of Lecture 2
- Key Points of Chapter 1 from CERT Book
- Technology used by
  - Business computer specialists
- Specialized techniques
  - Hidden data
  - Spyware/adware
  - Encryption methods
  - Protecting data
- Wireless technologies
- Firewalls
- Biometrics
- Demos: SMTP weakness, Recovery of data from floppy
- Conclusion

Lecture 2 Recap

- Technology used by
  - Military & Law Enforcement
- Defined *Forensics*—process using scientific knowledge to
  - Collect, analyze, and present evidence to the courts
  - Volatile versus persistent data
- Reading assignment (Chapters 1—2, Chapter on Network Security, Chapter 1 from CERT book)

Cyber Law (Chapter 1 CERT Book)

- SA & network security personnel as the first responder
  - Authority to monitor & Collect
    - 4th Amendment (Protection against unreasonable search & seizure)
  - Need to be aware of how routine admin tasks can affect (same way how law enforcement personnel are not lawyers, but enough about law)
  - Division of labor between law enforcement personnel and SAs

Laws that affect cyber security

- Authority to monitor & collect
  - Constitutional protection (limits government action)
    - 4th (enjoy a reasonable expectation of privacy) & 5th (protection against self incrimination) Amendment
  - Statutory Laws
    - Wiretap Act
      - Content and Non-content in DoD versus OSI Models
      - Prohibits interception of real-time communication (specifically content) unless there is an exception
      - Exception: SAs are allowed limited monitoring of content
      - Exception: Trespasser Exception
    - Pen/Trap and Trace
      - Prohibits interception of non-content
      - Provider Exception, Verification of Service (e.g. billing purposes), Consent
    - Stored Wired & Electronic Communication Act
      - Content versus non-content
      - Not real-time, stored
      - Provider cannot disclose contents
      - Content, logs, subscriber information

Federal Rules of Evidence

- Hearsay
  - Computer-generated records (not hearsay)
    - Admissible if a company logs everything
  - Computer-stored records (logs of driving related to business activity)
- Authentication
  - SA need to vouch for the action of generating a record, say running *netstat* command (and storing the results on some persistent storage)
  - Chain of custody
- Reliability
  - Information generated in the normal course of business
- Best evidence
  - Defines what is an "original"

Chapter 2 (cont.)

- Business Computer Forensic Technology
  - Remote monitoring (Spytech)
  - Intrusion detection system (IDS)
  - Theft recovery software
  - Basic forensic tools and techniques
  - Forensic services

Chapter 2 (cont.)

- Intrusion detection system (IDS)
  - Host based and network based
  - Many—2 billion dollar industry, e.g. sourcefire, snort (open source)
- Theft recovery software.
  - Loss of a PC results in
    - Hardware & software
    - Data (back ups)
    - Lost productivity
    - Cost of reporting and increase in insurance
  - Products
    - PC PhoneHome
    - Configure & give an email
    - Weaknesses
    - Loss of privacy

Chapter 2 (cont.)

- Forensic services typically provided
  - Lost password and file recovery
  - Retrieval of deleted and hidden files
  - File and email decryption (??)
  - Tracing Email to source
  - Internet activity (Net Nanny)
  - Usage policy and supervision
  - Remote monitoring
  - Honeypot (sting) operations

Business Computer Forensic Technology

- Remote Monitoring
  - Data Interception by Remote Transmission (DIRT) from Codex Data Systems
- Creating Trackable Electronic Documents (IDS)
- Theft Recovery for laptops
  - Loss of hardware, software, cost of recreating data, cost of reporting, increased insurance etc.
  - PC PhoneHome

Protection from worms/viruses

- Don’t open executable attachments (unless you know the sender and are expecting it). Most known extension are sandboxed
- Disable Windows Scripting Host
- Download from trusted sites
- Use anti-virus software
- Do regular back ups
- Education
- Use hashes and write protection for important documents
- Apply patches regularly

Specialized Forensic Techniques

- Legal Evidence
  - Find, preserve, and prepare evidence
  - Photograph, label wires and sockets
  - Capture the time a document was created, last opened/modified (% ls –t)
  - Sophisticated hackers usually cover their tracks (erase .history files, doctor logs etc.)
  - Use SHA to see a text file changed. To see what that change is use diff

Spyware/Adware

- Web email
- Primopdf
- Irfanview and Yahoo! Toolbar
- Have the potential to do serious damage
- Keyloggers

Security through obscurity

- In contrast to security by design
- From Wiki
  - use secrecy (of design, implementation, etc.) to provide security
  - may have theoretical or actual security vulnerabilities
  - Flaws are not known and attackers are unlikely to find them
- Netscape
  - Random number generation
- Lock manufacturers

Chapter 2 (cont.)

- Blackberry
  - SDK to
    - To take an image
    - examine the file system
  - Flash RAM
    - 65 ns read, x1000 times for write
    - 1 → 0 is easy, 0 → 1 requires erasure
    - Erasure in blocks of 64 KB
    - Erasure requires conditioning: force all 1 →0 first, and set all the bits in the block to 1. Hence slow
- Firewalls
  - Connection fully specified by source <IP, port> and destination <IP,port>
  - Well-known ports 0—1023, registered 1024—49151, 49152—65535 dynamic and private ports
- Biometrics