COMPUTER FORENSICS: A critical process in the incident response plan

Lecturer: Sue Foster
Week 5

Security product flaws attract attackers
MARCH 26, 2004 (COMPUTERWORLD)

The software vulnerability exploited by the Witty worm is only the latest in a growing list of flaws being discovered in the very products users invest in to safeguard their systems.

"This is a new realm of risk that users must confront: the security of security products," said Andrew Plato, president of Anitian Enterprise Security, a systems integration and consulting firm.

The Witty worm, reportedly damaged 15,000 to 20,000 computers worldwide, took advantage of a flaw involving the BlackIce and RealSecure intrusion-prevention products from Atlanta-based Internet Security Systems Inc. (ISS). The worm wrote random data onto the hard disks of vulnerable systems, causing the drives to fail and making it impossible for users to start up the systems.

The flaw was the result of a buffer-overflow condition in a function used to detect peer-to-peer traffic, said Chris Rouland, director of the X-Force security team at ISS.

Lecture objectives

- Describe Cyber crime
- Define Computer Forensics
- Relate computer forensics to Incident Response
- Discuss:
  - Forensic Process
  - Forensic Tools
  - Forensic Problems
- Understand Contemporary Issues in Computer Forensics
- The Future of Computer Forensics
KEYWORDS

- Cyber crime
- Computer forensics
- Incident response
- Incident classification
- Containment
- Steganography
- Ghosting

Computer Crime Today

- Crime Without Punishment
- Media Sensationalism
- Public Apathy
- Easy to Commit

What is Cyber Crime?

- A crime in which technology plays an important, and often a necessary, part.
  - The computer is:
    - the target of an attack
    - the tool used in an attack
    - used to store data related to criminal activity
Computer and Cyber Crime?

- Crimes directed against a computer
- Crimes where the computer contains evidence
- Crimes where the computer is used to commit the crime

Estonian Police Arrest Alleged Internet Bank Thief (1 April 2005)

- Estonian police have arrested a 24-year-old man suspected of stealing money from numerous bank accounts.
- The man allegedly infected victims' computers through email purporting to be about job offers; the malware he allegedly used stole personal information which could be used to access others' bank accounts.
- The malware used in the thefts managed to evade antivirus detection and erased evidence of itself after it had collected the desired information.

Further reading on the case:
http://news.scotsman.com/latest.cfm?id=4339692

The Nature of Computer Related Crime in Today's Organizations

Source: 2000 CSI/FBI Study
### Types of Cyber Crime

- Unauthorized Access
- Denial of Service
- Extortion
- Theft
- Sabotage
- Espionage
- Computer Fraud
- Embezzlement
- Copyright Violation
- Forgery and Counterfeiting
- Internet Fraud – “Imposter Sites”
- Identity fraud
- Child Pornography
- Stalking & Harassment
- Credit Card Fraud & Skimming
- Internet Fraud – “Imposter Sites”
- Identify fraud
- Child Pornography
- Stalking & Harassment
- Credit Card Fraud & Skimming

### Identity Theft

- According to CBS News, every 79 seconds a thief hacks into a computer, steals a victim's identity, and then goes on a buying spree.
- Identity theft is rapidly becoming one of the fastest growing serious crimes.

### Developing a Profile of an Intruder

- Crime scene analysis
  - how was access obtained?
  - What skills were required?
  - how did the intruder behave on the system?
    - Damage? Clean-up? Theft?
- Investigative psychology
  - motivation
  - personality type
Incident Response

Incident Response – Why is it Critical?

- Resolve the problem
  - Find out what happened
  - How it happened
  - Who did it
- Create a record of the incident for later use
- Create a record to observe trends
- Create a record to improve processes
- Avoid confusion
Elements of Incident Response

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow-up

Preparation

Without adequate preparation, it is extremely likely that response efforts to an incident will be disorganized and will cause considerable confusion among personnel.

Preparation limits the potential for damage by ensuring response actions are known and coordinated.

Identification

1. The process of determining whether or not an incident has occurred and the nature of an incident.
2. Identification may occur through the use of automated network intrusion equipment or by a user or system administrator.
3. Identification is a difficult process.
   - Noticing the symptoms of an incident is often difficult.
   - There are many false positives.
   - Noticing an anomaly should drive the observer to investigate further.
   - Training of staff is important.
Who can identify an Incident

- Users –
  - My system is slow, my mail is missing, my files have changed
- System support personnel –
  - Servers locked up, files missing, accounts added/deleted, weird stuff happening, anomalies in the logs
- Intrusion Detection Systems and Firewalls –
  - Automatically ID violations to policies

Possible Incident Classifications

- Unauthorized Privileged (root) Access
- Unauthorized Limited (user) Access
- Unauthorized Unsuccessful Attempted Access
- Unauthorized Probe
- Poor Security Practices
- Denial of Service (DOS) Attacks
- Malicious Logic code/software
- Hardware/Software Failure
- Infrastructure Failure
- Unauthorized Utilization of Services

Containment

The process of limiting the scope and magnitude of an incident.

As soon as it is recognized that an incident has occurred or is occurring, steps should immediately be taken to contain the incident.
**Containment - Example**

- Incidents involving using malicious code are common, and since malicious code incidents can spread rapidly, massive destruction and compromise of information is possible.

- It is not uncommon to find every workstation connected to a LAN infected when there is a virus outbreak.
  - Internet Worm of 1988 attacked 6,000 computers in the U.S. in one day.
  - LoveBug Virus affected over 10Million computers with damage estimated between $2.5B-$10B US
  - Kournikova worm affects still being analyzed

**Eradication**

- The process of removing the cause of the incident.
  - virus – anti-virus software is best
  - network may involve block/filter IP address at the router/firewall

- Ideal bring the perpetrators into legal custody and convict them in a court of law.
  - But there are more perpetrators to take their place
  - Must have legal evidence – computer forensics!!

**Recovery**

The process of restoring a system to its normal operating status

- Unsuccessful incidents –
  - ensure system operation and data not affected

- Complex and/or successful incidents –
  - May require complete restoration from known clean system backups.
  - Essential to assure the backups integrity and to verify restore operation was successful
Follow-Up

- Critical
- Helps to improve incident handling procedures
- Address efforts to prosecute perpetrators
- Activities Include:
  - Analyze the Incident and the Response
  - Analyze the Cost of the Incident
  - Prepare a Report
  - Revise Policies and Procedures

Computer Forensics

What is Computer Forensics?

Computer Forensics can be defined simply, as a process of applying scientific and analytical techniques to computer Operating Systems and File Structures in determining the potential for Legal Evidence when an incident has occurred.
Why is Evidence important?

- In the legal world, Evidence is EVERYTHING.
- Evidence is used to establish facts.
- The Forensic Examiner is not biased.

Investigative Axiom

Treat every incident as if it will end up in a criminal prosecution.

Figure 1: Research Boundary on the Crime to Court Investigation Path
Who needs Computer Forensics?

- The Victim!
- Law Enforcement
- Insurance Carriers
- Ultimately the Legal System
Reasons for a Forensic Analysis

- ID the perpetrator.
- ID the method/vulnerability of the network that allowed the perpetrator to gain access into the system.
- Conduct a damage assessment of the victimized network.
- Preserve the Evidence for Judicial action.

Types of Computer Forensics

- Disk Forensics
- Network Forensics
- E-mail Forensics
  - Email spoofing
- Internet (Web) Forensics
- Source Code Forensics
Goals of an Investigation

- To ensure that all applicable logs and evidence are preserved
- To understand how the intruder is entering the system
- To obtain the information you need to justify a trap and trace of the phone line the intruder is using or to obtain a subpoena to obtain information from an ISP
- To discover why the intruder has chosen the computer
- To gather as much evidence of the intrusion as possible
- To obtain information that may narrow list of suspects
- To document the damage caused by the intruder
- Gather enough information to decide if law enforcement should be involved.

Immediate Objective:

**PRESERVE THE EVIDENCE !!!**

- Begin a traceback to identify possible log locations
- Contact system administrators on intermediate sites to request log preservation
- Contain damage
- Collect local logs
- Image disks on victim computers
Building an Incident Hypothesis

- Start with witness accounts
- Consider how the intruder could have gained access
  - eliminate the obvious
  - use logs and other physical evidence
    - consider the skill level or inside knowledge required
- Create mirror images of affected computers

Building an Incident Hypothesis

- Develop a profile of the intruder
- Reconstruct the path of the intruder to the victim computer – Back trace
- Recreate the incident in the lab
  - use real mirrors whenever possible
- Consider alternative explanations
  - test alternatives

Incident Reconstruction

- Physical
  - use mirrors of the actual involved systems
  - useful for single computers
- Logical
  - use similar systems
  - useful for networks where you have access to the entire network
- Theoretical
  - hypothesize intermediate computers
  - necessary when you can’t access all involved computers
Back Tracing

- Elements of a back trace
  - end points
  - intermediate systems
  - e-mail and packet headers
  - logs
- Objective: retrace steps to the actual dial in
- The only messages that can’t be back traced are those using a true anonymizer and those where no logs are present

Enabling Relationships

![Diagram showing relationships between an intruder’s laptop, ISP, router, intermediate host, and victim.]

Forensics Process

- Preparation
- Protection
- Imaging
- Examination
- Documentation
Preparation

- Confirm the authority to conduct analysis/search of media.
- Verify the purpose of the analysis and the clearly defined desired results.
- Ensure that sterile media is available and utilized for imaging. (i.e., Free of virus, Non-essential files, and verified before use.)
- Ensure that all software tools utilized for the analysis are tested and widely accepted for use in the forensics community.

Electronic Communications Privacy Act (ECPA) 1986 (US)

- Owner may intercept communications between an intruder and owner's computer system.
- Owner may provide others with access to use that computer to communicate with other computer systems:
  - make routine backups and perform other routine monitoring
  - intercept with prior consent of the user
  - intercept portions of communications necessary to determine origin and destination
  - intercept where necessary to protect owners rights or property
  - disclose to law enforcement any communications inadvertently discovered which reveal criminal activity

Protection

- Protect the integrity of the evidence.
- Maintain control until final disposition.
Imaging

- Utilize disk “imaging” software to make an exact image of the target media. Verify the image.
- When conducting an analysis of target media, utilize the restored image of the target media; *never* utilize the actual target media.

Examination

- The Operating System
- Services
- Applications/processes
- Hardware
- LOGFILES!
- System, Security, and Application
- File System

Examination (Cont)

- Deleted/Hidden Files
- Software
- Encryption Software
- Published Shares/Permissions
- Password Files
- Security incident detection system
- Network Architecture
Documentation

- Document **EVERYTHING**
- Reason for Examination
- “The Scene”
- Utilize Screen Capture/Copy Suspected files
- All apps for Analysis/apps on Examined system.

Forensic Tools

- Forensic Tool Kit
  (Manual/software)
- Forensic Computer System
- Forensic Software

List Directories and Files

- Create Hierarchical Directory Listing (Tree)
- Identify Suspect Files
- Inventory All Files on the Disk
- Search Communications Programs
- Registry Files
- Last Files Accessed
- Document Association

Reference: Inspecting your Solaris system and network logs for evidence of intrusions:
http://www.cert.org/security-improvement/implementations/020.01.html
Identify Suspect Files

- File Name Search based on Case Characteristics
- Key Word Search based on Case Characteristics
- Modified File Extensions that Do Not Match the File Type
- Hidden or Deleted Files

Hidden and Obscure Data

- Hidden File Attributes
- Hidden Directories
- Temporary Directories
- Deleted Files
- Slack Space
- Unallocated Space
- Swap Space
- Steganography

Steganography

- The Art of Hiding Communications
- While Encryption Conceals the Data, Steganography Denies the Data Exists
- Files Can Be Hidden within an Image
- Disguising Data as Innocent Text
S-Tools

- Hides Data inside Images, Audio Files and Slack Space

Ghosting

- White letters on a white background, or black letters on a black background.
Cluster Analysis

- Cluster Analysis Criteria
  - Content, Location and Condition
  - Identifies System Usage & History
    - Initial Load of the System
    - Defragmentation
      - "Repacks" data files w/o Changing Date/Times
      - System Wipes and Reloading
        - All Slack Space and Unallocated Blocks set to Zero
        - All Date/Times close to the same

Evidence Protection

- Transparent Static Shielding Bags
  - Provides shielding from electrostatic discharge by safely enveloping static sensitive devices in a humidity-independent Faraday cage. The nickel shielding layer creates a Faraday type shield. Meets MIL-B-81705 and DoD-STD-1686A

- Foam-Filled Disk Transport Box
- EMF Warning Labels
Contemporary Issues in Computer Forensics

- Criminal Justice System is not Prepared to Handle High-Tech Crime
  - Shortage of Trained Investigators & Analysts
  - Lack of Forensic Standards
- Too Much Data!
  - Large Disk Drives and Disk Arrays
  - High Speed Network Connections
- Issues Relating to Time

The Future Forensics

- Crimes and Methods to Hide Crimes are becoming more Sophisticated, thus Investigators and Analysts must become more Technical
  - Specialist are Needed
  - More Training is needed in both the Public and Private Sectors
- Encryption will Continue to be an Issue, but Only Time will Tell

The Future Forensics

- Forensic Tools
  - Must Become Automated
  - Forensic Search Engines Must better developed
  - Better Network Analysis Tools need to be Developed
Conclusions

- Computer forensics is an integral function within incident response
- Processes are the most important aspects of computer forensics
- The future of cyber crime will lead to an increased need for computer forensic capabilities

REVIEW QUESTIONS

- DESCRIBE THE IMPORTANCE OF COMPUTER FORENSICS
- WHY HAS COMPUTER FORENSICS BECOME SUCH A MAJOR CONCERN?

Additional readings

- ONCTek List of possible Trojan/Backdoor Activity http://www.onctek.com/trojanports.html
- US CODE COLLECTION http://www4.law.cornell.edu/uscode/18/2701.html