



An overview of IT Security Forensics

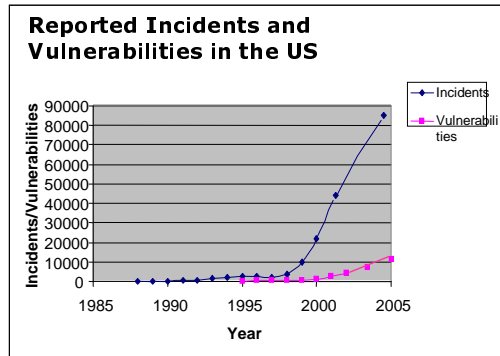
Manu Malek, Ph.D.
Department of Computer Science
Stevens Institute of Technology
mmalek@ieee.org
www.cs.stevens.edu/~mmalek
2/20/07

Outline

- ❖ Growing Threats/Attacks
- ❖ Need for Security Forensics
- ❖ Basic Methodology
- ❖ Forensic Tools
- ❖ A Sample Tool

Growing Threats/Attacks

- ❖ Cyber attacks are on the rise
 - An increase of over 30 times during the past 5 years
 - An increase of 10 times during the past 3 years
- ❖ *Cyberterrorism:*
The potential exists for attackers to break into computer networks controlling sensitive processes.



Adopted from www.cert.org

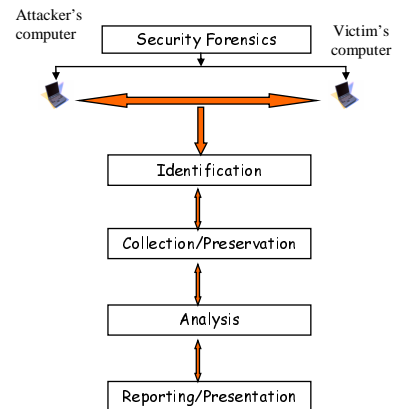
Trends Affecting Safe Internet Usage

- ❖ Faster discovery of vulnerabilities
- ❖ Automation and rising speed of attack tools
 - Scanning for vulnerable systems
 - Coordinated attack tools
- ❖ Increasing sophistication of attack tools
 - Dynamic behavior
 - Anti-forensics
- ❖ Increasing permeability of firewalls



What is Security Forensics?

- ❖ **Forensic:** *Belonging to, or used in, public debate or court of law*
- ❖ **Security Forensics:** Application of science and engineering to dealing with evidence stored on computers and network devices
- ❖ It is the process of
 - Identifying,
 - Collecting and preserving,
 - Analyzing, and
 - Reporting and presenting digital evidence in a manner that is legally acceptable.

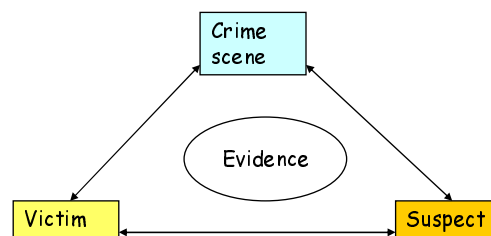


Need for Security Forensics

- ❖ Forensic methods are used to
 - Determine root cause of events
 - Support litigation
- ❖ Examples:
 - Today's corporate environment requires preparation for possibilities of future litigation, e.g., for
 - Wrongful termination claims
 - Intellectual property claims
 - Antitrust cases
 - Law enforcement agencies use computer forensics in civil and criminal suits

Locard's Principle and Continuity of Offense

- ❖ **Locard's Exchange Principle:** When any two objects come into contact, there is transference of material from one object to another.
- ❖ **Continuity of offense:** Attribute the crime to its perpetrator by providing compelling links between the suspect offender, victim, and crime scene.



IT Requirements for Forensics

- ❖ The following capabilities are needed to support Computer Forensics:
 - Being able to collect relevant information from systems
 - Being able to positively identify users who log on to systems
 - Being able to handle challenges to data ownership or audit trails found on a system
- ❖ Examples of activities to meet these requirements:
 - Logging user actions
 - Logging system and network events
 - Maintaining time servers and standard time settings
 - Giving each new employee a computer with a forensically clean disk and a standard set of applications
 - Duplicating all the data on an employee's computer before he/she is informed of job termination

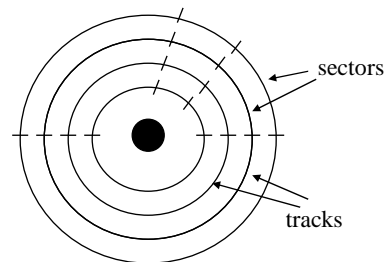
Forensic Data Collection in Client Computers

- ❖ Most operating systems provide significant logging capabilities.
 - Windows systems (2000/NT/XP) store log files in the directory `%systemroot%\system32\config\`
 - In UNIX, information about running processes is usually stored in `var/log/syslog`
- ❖ Device logs; for example, one can find out if
 - A USB device has been used
 - A CD burner has been used
 - A file has been printed
- ❖ Protecting logs
 - Attackers could delete or modify logs
 - Logs should be protected

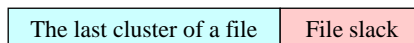
Hidden Evidence

- ❖ Evidentiary data may not be readily observable.
- ❖ Evidence could be in
 - Deleted files
 - Encrypted files
 - Files hidden in other files
 - Files in parts of the hard drive that are not readily exposed:
 - File slack
 - ATA "Protected Area"

A Disk Platter



A sector



Network-based Evidence

- ❖ Network monitoring can be performed to collect evidence:
 - **Event monitoring**: collecting network events, such as IDS alerts, network health monitoring alerts
 - **Trap-and-trace monitoring**: transaction data such as protocol flags
 - **Full-content monitoring**: collecting raw packets
- ❖ Network-based evidence can be found at endpoints and intermediate systems, such as
 - Authentication servers
 - Router logs
 - Firewall logs
 - Event logs from IDSs
 - Caller ID systems ...

Forensic Tools

- ❖ Many forensic tools and applications exist, e.g., for
 - Hard disk duplication
 - Text and file searching
 - Internet history analysis
 - Analysis of email files
 - Analysis of data stores
 - Network forensics
- ❖ Some popular tools:
 - *EnCase* for drive forensics
 - *E-Trust* for industrial espionage cases
 - *Forensic Toolkit* (FTK)
 - *ProDiscover*
- ❖ Hardware and software-based key loggers can collect key strokes for specified periods of time.