Incident Handling

Week 4: Incidents, Evidence and the Law

George Berg & Jagdish S. Gangolly
University at Albany
Road Map

• What is digital evidence?
  – What are different types of evidence?
  – What are their desirable characteristics?
• What is the legal environment in which incidents are handled?
• How to prevent and detect incidents?
• What is the sequence of events in responding to incidents?
• What are the principles governing gathering of evidence?
Digital Evidence

- Some definitions of digital evidence:
  - “Any data that can establish that a crime has been committed, or can provide a link between a crime and its victim or a crime and its perpetrator”
    - (Casey, 2000)
  - “Any information of probative value that is either stored or transmitted in a digital form”
    - (Standard Working Group on Digital Evidence - SWGDE)
  - “Information stored or transmitted in binary form that may be relied upon in court”
    - (International Organisation of Computer Evidence)
Types of Evidence

- Physical evidence (computers, network equipment, storage devices, ...)
- Testimonial evidence
- Circumstantial evidence
- Admissible evidence (evidence that a court accepts as legitimate)
- Imadmissible evidence
  - Hearsay evidence
Hearsay Evidence: Exception

- “A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.”
Characteristics of Evidence

- **Authenticity** (unaltered from the original)
- **Relevance** (relates crime, victim and perpetrator)
- **Traceability** (audit trail from the evidence presented back to the original)
- **Complete** (presents total perspective on the crime. Ideally, should include exculpatory evidence)*
- **Reliable** (one should not be able to doubt the authenticity and traceability of the evidence collection and chain of custody)
Characteristics of Evidence

• **Believable** (jury should be able to understand the evidence)
Legal Environment

• Fourth Amendment (US Constitution)
• Computer Fraud and Abuse Act 1996
• Health Industry Portability and Accountability Act, 1996
• Wiretap statute (18 U.S.C. Chap 119)
• Fraud & Related Activity in Connection with Access Devices (18 U.S. Part I Chap 47 § 1029)
• Digital Millennium Copyright Act
• PATRIOT Act, 2001
Fourth Amendment

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
Fourth Amendment

• Protection of Property (Olmstead v. US, 1928)
  – Wiretap of private phone conversation is not “search” since there is no intrusion into one’s home.

• Protection of People (Katz v. US, 1967)
  – What a citizen seeks to preserve as private, even in an area accessible to the public may have protection from “search and seizure.”

• Protection of Privacy (Crime Control & Safe Streets Act, 1968)
  – Wiretap/microphone surveillance requires warrant based on probable cause.
Computer Fraud and Abuse Act, 1984

- Designed mainly to protect national security, financial/commercial information, medical, interstate communication systems
- Prohibits DoS attacks causing losses of $10,000 or more
- Allows civil action by victims against perpetrators
- Cases:
  - Internet worm (US v. Morris, 1991)
  - Stealing and publication of Bell South enhanced 911 system (US v. Riggs, 1990)
Health Industry Portability and Accountability Act, 1996

- “HIPAA”
- Safeguarding of health information
- Requires healthcare providers to have adequate security standards
- Impact of the law is still not very clear
Wiretap statute (18 U.S.C. Chap 119)

• “any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce”
Fraud & Related Activity in Connection with Access Devices (18 U.S. Part I Chap 47 § 1029)

- Covers
  - credit cards,
  - computer passwords, and
  - all access codes/devices.

- Covers
  - trafficking in,
  - counterfeiting,
  - producing,
  - using,
such devices without authorization.
Digital Millennium Copyright Act

• “DMCA”

• Criminalizes making, distributing, or using tools (software) to circumvent technological protection measures.

• Criminal penalties (up to 5 years in prison and $500,000 in fines for first offense).
Patriot Act, 2001

• PATRIOT (“Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”)
  – Expands government’s ability to use technology as a surveillance and data collection tool.
  – Gives federal officials authority to track and intercept communications.
  – Provides Secretary of Treasury power to combat money-laundering.
  – Expands ability of government to conduct secret searches.
  – FBI can access business records about individuals without showing evidence of a crime.
Other Relevant Laws

- 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers
Other Relevant Laws


Other information: (DOJ Manual)

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

Prevention & Detection of Incidents

• Need for assessment of risk and development of metrics and systems for early warning of incidents.
• Development of Security Policies and review procedures.
• Development of systems and protocols for reporting of incidents and incident handling (including evidence handling).
• Identification, Development, and implementation of controls to enforce the policies.
• Development and implementation of a system for monitoring operations (including operations of the control system).
Prevention & Detection of Incidents

• Policy Framework for Interpreting Risk in eCommerce Security (PFIRES)

(http://www.cerias.purdue.edu/news_and_events/events/securitytrends/1999_pfires.pdf)
Prevention & Detection of Incidents

• Importance of recognizing signs of incidents as they occur.
  – If not recognized then, important evidence may not be available later, and may be more difficult to catch the perpetrator.

• Need to assess vulnerabilities continuously, since new ones may emerge.

• Important to have a good understanding of what is the normal behavior of the system.

• Importance of a Computer Security Incident Response Team (CSIRT)
  – (See CERT’s CSIRT Handbook)
Typical Sequence of Events in Incident Response (RFC2196 Model)

- RFC 2196 “Site Security Handbook”
  - [http://www.faqs.org/rfcs/rfc2196.html](http://www.faqs.org/rfcs/rfc2196.html)

- Incident Management

- Sequence of Events
  1. Abnormal/unexpected behavior detected
  2. Preparation
  3. Detection
  4. Containment
  5. Eradication
  6. Recovery
  7. Follow-Up
Typical Sequence of Events in Incident Response (RFC2196 Model)

1. Identification of the incident
   1. Is it real? (False alarms)
   2. Determine the scope of the incident
   3. Assess damage

2. Notification of incident
   1. Whom to notify,
   2. what to document,
   3. choice of language.
Typical Sequence of Events in Incident Response (RFC2196 Model)

3. Protection of evidence
   1. Audit records
   2. Time-tagged actions taken in the investigation
   3. Details of all external conversations
   4. Collecting evidence

4. Containment
   1. Decision whether to shut down the system
   2. How to shut down the system without losing or corrupting the evidence
Typical Sequence of Events in Incident Response (RFC2196 Model)

5. **Eradication**
   1. Collect all evidence before this step
   2. Removal of the vulnerability that caused the incident

6. **Recovery from clean backups**

7. **Follow up (Post mortem of the incident)**
Evidence Collection Principles

• Maintain chain of custody of the evidence.
• Acquire evidence from volatile as well as non-volatile memory without altering or damaging original evidence.
• Maintain the authenticity and reliability of evidence gathered.
• No modification of data while analyzing it.
Maintaining Chain of Custody

• Movement of evidence from place to place must be documented.
• Changing of hands in custody of the evidence must be documented.
• There must be no gaps in the custody of the evidence.
Volatile & Non-volatile memory

• Places where evidence may reside
  – Memory
    • RAM
    • Virtual memory pages written to the hard drives
  – Hard drives
    • File systems
    • Parts of disk with no file system loaded.
Volatile & Non-volatile memory

• Memory:
  – In MS-Windows 2000,
    • setting up the Registry to enable capturing memory.dmp manually
    • Using Dumpchk.exe to generate memory dump
  – In unix systems,
    • using /etc/sysdump to generate a live dump of /dev/mem, and
    • using /etc/crash to analyze the dump
Volatile & Non-volatile memory

• Hard Drives
  – Imaging: Non-destructive Sector-by-Sector copy of the drive that does not require the machine to be booted
  – NIST requirements for imaging tools:
    • Tool makes Bit-stream copy or image of the disk or partition if there are no access errors
    • No altering of the disk by the tool
    • Tool must access both IDE and SCSI
    • Tool must verify the integrity of the image file
    • Tool must log I/O errors, and create a qualified bit-stream duplicate identifying the areas of bit-stream in error
    • Tool’s documentation must be correct
    • Notify user if source disk is larger than destination disk
Volatile & Non-volatile memory

• Some tools:
  – Linux dd (www.redhat.com)
  – SnapBack DatArrest (www.snapback.com)
Authenticity & Reliability of Evidence Gathered

• **Time Synchronization problems in networks**
  – If the times on various machines are not synchronized, the evidence collected may not have strength.
  – Network Time Protocol (NTP) supported on Unix, Linux, but not supported in Windows.
  – However there are third-party tools such as those found at
    • [www.oneguycoding.com/automachron](http://www.oneguycoding.com/automachron)
    • NIST Internet Time Service
      [www.nist.gov/timefreq/service/its.htm](http://www.nist.gov/timefreq/service/its.htm)
    • [www.pawprint.net/wt](http://www.pawprint.net/wt)
Authenticity & Reliability of Evidence Gathered

- **Time Stamping**
  - Once the system is compromised, the perpetrator will alter the logs to confuse the investigator
  - Digital time stamping service can be used
    - [www.datum.com](http://www.datum.com)
    - [www.evertrust.com](http://www.evertrust.com)
  - Use of Tripwire Monitoring & Reporting Software to monitor changes
Synopsis

• What is digital evidence?
  – What are different types of evidence?
  – What are their desirable characteristics?
• What is the legal environment in which incidents are handled?
• How to prevent and detect incidents?
• What is the sequence of events in responding to incidents?
• What are the principles governing gathering of evidence?