

Incident Handling

Week 4: Incidents, Evidence and the Law

George Berg & Jagdish S. Gangolly
State University of New York at Albany

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

1

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?

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

2

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 - SWEDE)
- “Information stored or transmitted in binary form that may be relied upon in court” (International Organisation of Computer Evidence)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

3

Types of Evidence

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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

4

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.”

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

5

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)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

6

Characteristics of Evidence

- Believable (jury should be able to understand the evidence)
-

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

7

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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

8

Fourth Amendment (US Constitution)

“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.”

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

9

Fourth Amendment (US Constitution)

- 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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

10

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)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

11

Health Industry Portability and Accountability Act, 1996

- Safeguarding of health information
- Requires healthcare providers to have adequate security standards
- Impact of the law not very clear

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

12

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”

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

13

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 authorisation

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

14

Digital Millennium Copyright Act

- 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)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

15

Patriot Act, 2001

- 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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

16

Other Laws

- [18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices](#)
- [18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers](#)
- [18 U.S.C. § 1362. Communication Lines, Stations, or Systems](#)
- [18 U.S.C. § 2510 et seq. Wire and Electronic Communications Interception and Interception of Oral Communications](#)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

17

Other Laws

- [18 U.S.C. § 2701 et seq. Stored Wire and Electronic Communications and Transactional Records Access](#)
- [18 U.S.C. § 3121 et seq. Recording of Dialing, Routing, Addressing, and Signaling Information](#)

Other information: (DOJ Manual)

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

<http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm>

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

18

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)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

19

Prevention & Detection of Incidents

- Policy Framework for Interpreting Risk in eCommerce Security
(http://www.cerias.purdue.edu/news_and_events/events/securitytrends/1999_ptires.pdf)



5/3/2004

Incident Handling (G. Berg & J. Gangolly)

20

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 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 Computer Security Incident Response Team (CSIRT) (See CSIRT Handbook)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

21

Typical Sequence of Events in Incident Response (RFC2196 Model)

RFC 2196 and Incident Management

(<ftp://ftp.isi.edu/in-notes/rfc2196.txt>)

0. Abnormal/unexpected behavior detected
1. Preparation
2. Detection
3. Containment
4. Eradication
5. Recovery
6. Follow-Up

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

22

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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

23

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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

24

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)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

25

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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

26

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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

27

Volatile & Non-volatile memory

- Places where evidence may reside
 - Memory
 - Hard drives
 - File systems
 - Parts of disk with no file system loaded
- 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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

28

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 make 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 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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

29

Volatile & Non-volatile memory

- Some tools:
 - Linux dd (www.redhat.com)
 - SnapBack DatArrest (www.snapback.com)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

30

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
 - NIST Internet Time Service
www.nist.gov/timefreq/service/its.htm
 - www.pawprint.net/wt

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

31

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
 - www.evertrust.com
 - Use of Tripwire Monitoring & Reporting Software to monitor changes

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

32

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?

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

33