

Incident Handling

Week5:How to Handle Incidents and Evidence

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

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

1

Road Map

- How to handle incidents?
 - Types of incidents based on severity
 - How to recognise them
 - Whether to report them
 - Actions required to maintain readiness to handle incidents
 - Actions to take at the scene of the incident
 - Pull the plug? Turn off the machine? Live forensics?

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

2

Road Map

- How to handle evidence?
 - What to search/seize?
 - What kind of evidence to gather? How?
 - Documenting the evidence gathered
 - How to maintain the authenticity of evidence?

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

3

How to handle incidents?

- What are the types of incidents from the viewpoint of response? How they are recognized?
- Whether to report incidents, and to whom to report?
- What actions are required to maintain readiness to handle incidents?
- What actions to take at the scene of the accidents?
- What actions to take to protect evidence?
- What evidence to collect and how to collect?

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

4

Types of incidents based on severity

- LOW
 - Loss of passwords, unauthorised sharing of passwords, successful/unsuccessful scans/probes, hardware misuse,...
- MEDIUM
 - Property destruction, illegal download of music/files or unauthorised software, unauthorised use of system for personal data, acts by disgruntled employees, illegal hardware access/tress pass, theft (minor)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

5

Types of incidents based on severity

- HIGH
 - Child pornography, pornography, personal theft, property destruction, break-in, illegal software download, malicious code (viruses, worms, trojan horses, malicious scripts,...), changes to system hardware, software, or firmware, violation of law.

Source: *Incident Response: Computer Forensics Toolkit*, Douglas Schweitzer, (John Wiley, 2003)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

6

Types of incidents & How to recognize them

- End user detected incidents
- Application detected incidents
- System detected incidents

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

7

End user detected incidents

- Unavailability of web pages
- Download of file containing virus/worm
- Abnormal behavior of web site
- Spam
- Distribution of pornography
- Unusual request of personal information (ebay, Nigerian scams)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

8

Application detected incidents

- Abnormal behavior of an application
- Inappropriate use of application (eg., unauthorised access)
- Unauthorised change of data (eg., defacement of web pages, alteration of data,...)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

9

System detected incidents

- Detected by intrusion detection systems
- Detected by analysis of firewall logs
- Viruses/worms detected by servers
- Unavailability of servers (DoS attacks)
- Lack of remote availability of the system
- Detection of abnormal changes by monitoring software (eg., tripwire)
- Unauthorised access of servers,...

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

10

Whether to report incidents?

- Depends on the party: users, system administrators
 - Users: In their interest to report the incident, usually to the “help desk”
 - System administrators: Report to CSIRT (Computer Security Incident Response Team) in the Company.

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

11

Whether to report incidents?

- Report to Law Enforcement?
 - Consult lawyers if an illegal act has occurred and if there are reporting responsibilities
 - Reporting to law enforcement changes the character of the evidence handling process.
 - Evidence can be subpoenaed by courts
 - Perpetrators and their lawyers can get access to it in the trial
 - Evidence gathering process and all actions and documentation of the investigations may also be accessible to the other party during litigation.

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

12

What actions are required to maintain readiness to handle incidents?

- Acceptable use policies
- Access control policies
- Protocols for handling incidents
- Education of all personnel on dealing with incidents
- Incident handling toolkits (hardware and software)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

13

What actions are required to maintain readiness to handle incidents?

- System backups
- Computer Security Incident Response Team (CSIRT)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

14

Incident handling toolkits

- Hardware:
 - Large capacity IDE & SCSI Hard drives, CD-R, DVR drives
 - Large memory (1-2GB RAM)
 - Hubs, CAT5 and other cables and connectors
 - Legacy hardware (8088s, Amiga, ...) specially for law enforcement forensics
 - Laptop forensic workstations

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

15

Incident handling toolkits

- Software
 - Viewers (QVP <http://www.avantstar.com/>, ThumbsPlus <http://www.thumbsplus.de/>)
 - Erase/Unerase tools: Diskscrub/Norton utilities
 - CD-R, DVR utilities
 - Text search utilities (dtsearch <http://www.dtsearch.com/>)
 - Drive imaging utilities (Ghost, Snapback, Safeback,...)
 - Forensic toolkits
 - Unix/Linux: TCT The Coroners Toolkit/ForensiX
 - Windows: Forensic Toolkit

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

16

Forensic Boot Floppies

- Disk editors (Winhex,...)
- Operating systems
- Forensic acquisition tools (DriveSpy, EnCase, Safeback, SnapCopy,...)
- Write-blocking tools (FastBloc <http://www.guidancesoftware.com>) to protect evidence.

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

17

Policies

- Who can add or delete users?
- Who can access machines remotely
- Who has root level access to what resources (SetUID and sudo privileges)
- Control over pirated software
- Who can use security related software (network scanning/snorting, password cracking, etc.)
- Policy on internet usage

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

18

System backups

- Systems backups help investigation by providing benchmarks so that changes can be studied
- Unix:
 - dump: dump selected parts of an object file
 - cpio: copy files in and out of cpio archives
 - tar: create tape archives and add or extract files
 - dd: Convert and copy a file

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

19

System backups

- Windows:
 - Programs | Accessories | System Tools | Backup
 - NTBACKUP: Part of NT Resource kit
 - Backup : From disk to disk

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

20

What actions to take at the scene of the accidents?

- Pull the plug? Turnoff the machine?
Live forensics?
- What to search/seize?
- What kind of evidence to gather?
How to gather the evidence?
- How to maintain authenticity of the evidence?

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

21

Pull the plug? Turnoff the machine? Live forensics?

- By pulling the plug you lose all volatile data. In unix system, you may be able to recover the data in swap space
- Perpetrator may have predicted the investigation, and so altered system binaries
- You can not use the utilities on the live system to investigate. They may have been compromised by the perpetrator

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

22

What to search/seize?

- Public investigations (criminal, usually by law enforcement agencies) vs. Corporate investigations.
- Public investigations, with search warrants, can seize all computers & peripherals, but fourth amendment provides protection
- Corporate investigators may not have the authority to seize computers, but may only allow one to make bit-stream copies of drives

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

23

What kind of evidence to gather? How?

- Secure the scene with yellow tape barriers to prevent bystanders from entering or interfering with investigation.
- The computer is just one of a number of types of evidence to be gathered
- DNA evidence from keyboard
- Fingerprint evidence (AFIS: Automated Fingerprint Identification System)
- Fingerprints of all people who had access to the crime scene

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

24

What kind of evidence to gather? How?

- No one to examine the computer before the bit stream image of the hard drive has been captured
- Follow the standards outlined in DOJ Manual
- Keep journal on all significant activities, people encountered.
- Good idea to carry a tape recorder, and a still pictures camera
- Usually not a good idea to video tape the scene. The defendant's attorney may have access to it during trial.

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

25

What kind of evidence to gather? How?

- If the computer is on,
 - capture information on the processes, save data on all current applications, photograph all screens.
 - After saving all active files (preferably on external media, but if necessary to save on seized computer, save with a new name to avoid confusion), you can shut down the system.
- If the computer is off, you can acquire the evidence on hard drives (you will have lost the data in volatile memory)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

26

What kind of evidence to gather? How?

- Tagging and bagging evidence (including software/hardware documentation)
- Precautions:
 - Grounding wristbands, static electricity resistant floor mats
 - Mark location of collected evidence
 - Carry response kit (laptop, flashlight, digital camera, IDE 40-to-44 pin adapters, computer toolkit, dictation recorder, evidence bags, labels, tags, tape, marking pens, floppy disks, evidence log forms,...)

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

27

Documenting the evidence gathered

- Maintain either single or multiple evidence forms to document evidence gathered
- The forms should include: Case number/name, Nature of the case, for each item its description (model/serial numbers, manufacturer), case investigator, investigator recovering the evidence, location of original evidence,

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

28

How to maintain authenticity of the evidence?

- Maintaining authenticity provides assurance to the jury that the evidence is reliable and has not been tampered with.
- Authenticity is provided by cryptographic checksums (message digests or fingerprints).
- MD5 and SHA are two common hash algorithms used. They provide a fingerprint of the evidence gathered.

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

29

How to maintain authenticity of the evidence?

- Executable for MD5 algorithm can be downloaded from <http://www.etree.org/software.html> for various operating systems.
 - Example: In unix systems, if you want the MD5 digest of the files /etc/passwd and /etc/services files, you would
 - Cat /etc/passwd and /etc/services >file
 - Md5sum file > file.md5
- Such algorithms are subject to cryptographic attack. Therefore it is important to provide some redundancy.

5/3/2004

Incident Handling (G. Berg & J. Gangolly)

30

How to maintain authenticity of the evidence?

- Some software such as Tripwire compute hash values using multiple algorithms so that even if one algorithm becomes susceptible to attack, authenticity can be proven using other algorithms
- Whenever a copy of the evidence is to be produced, the authenticity of the copy can be shown by re-computing the hash value and comparing with the original

Synopsis

- How to handle incidents
- How to handle evidence