Incident Handling

Week 5

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

• How to handle incidents?
  – Types of incidents based on severity.
  – How to recognize 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?
    • Power down the machine?
    • Or do live forensics?
Road Map

• How to handle evidence?
  – What to search/seize?
  – What kind of evidence to gather?
    • How to gather it?
  – Documenting the evidence gathered.
  – How to maintain the authenticity of evidence?
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?
Types of Incidents Based on Severity

- Incidents can be grouped by their severity.
  - High
  - Medium
  - Low.
- The grouping is based on their impact
Types of Incidents Based on Severity

• LOW
  – Loss of passwords,
  – Unauthorized sharing of passwords,
  – Successful/unsuccessful scans/probes,
  – Hardware misuse,
  – Etc.
Types of incidents based on severity

• MEDIUM
  – Minor property destruction,
  – Illegal download of music/files or unauthorized software,
  – Unauthorized use of system for personal data,
  – Acts by disgruntled employees,
  – Illegal hardware access/trespass,
  – Theft (minor).
Types of incidents based on severity

• HIGH
  – Child pornography,
  – Pornography,
  – Personal theft,
  – Major 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.
Types of incidents & How to Recognize Them

• End user detected incidents.
• Application detected incidents.
• System detected incidents.
End User Detected Incidents

- Unavailability of web pages.
- Abnormal behavior of web site.
- Downloading a file containing virus/worm.
- Spam.
- Distribution of pornography.
- Unusual request of personal information (e-bay, Nigerian scams).
Application detected incidents

- Abnormal behavior of an application
- Inappropriate use of application (*e.g.* unauthorized access)
- Unauthorized change of data (*e.g.* defacement of web pages, alteration of data, …).
System Detected Incidents

- Detected by intrusion detection systems (IDSs).
- 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 (e.g. tripwire).
- Unauthorised access of servers, ...
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.
  – Information Security Officers: Incident response policies, regulations and legal requirements.
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.
    • Alleged perpetrators and their lawyers can get access to it in the trial.
    • The evidence gathering process and all actions and documentation of the investigations may also be accessible to the other party during litigation.
What Actions are Required to Maintain Readiness to Handle Incidents?

- Policies
- Response Preparation
What Actions are Required to Maintain Readiness to Handle Incidents?

• Policies
  – Acceptable use policies.
  – Access control policies.
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.
What Actions are Required to Maintain Readiness to Handle Incidents?

• Response Preparation
  – Computer Security Incident Response Team (CSIRT).
  – Protocols for handling incidents.
  – Education of all personnel on dealing with incidents.
  – Incident handling toolkits (hardware and software).
  – System backups.
Incident handling toolkits

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

• Software
  – Viewers (QVP http://www.avantstar.com/, ThumbsPlus http://www.thumbsplus.de/)
  – Erase/Unerase tools: Diskscrub/Norton utilities
  – CD-R, DVD-R 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
Forensic Boot Floppies

• Bootable
  – Contains the operating system
• Disk editors (Winhex, …)
• Forensic acquisition tools (DriveSpy, EnCase, Safeback, SnapCopy,…)
• Write-blocking tools (FastBloc http://www.guidancesoftware.com) to protect evidence.
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
System backups

- Windows:
  - Programs\Accessories\System Tools\Backup
  - NTBACKUP: Part of NT Resource kit
  - Backup : From disk to disk
What actions to take at the scene of the accidents?

- Pull the plug? Power down the machine? Or do live forensics?
- What to search/seize?
- What kind of evidence to gather?
  - How to gather the evidence?
- How to maintain authenticity of the evidence?
Pull the plug?

• By pulling the plug you lose all volatile data.
  – In Unix systems, you may be able to recover the data that was in the swap space for virtual memory.
Pull the plug?

• 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.
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 the 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.
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.
- Evidence from keyboard (fingerprint, DNA?).
- Fingerprints of all people who had access to the crime scene.
What kind of evidence to gather?

How?

• No one is 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.
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.
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, …).
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,
  – Name of the investigator recovering the evidence,
  – Location of original evidence,
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.
How to maintain authenticity of the evidence?

• Executable for MD5 algorithm can be downloaded from [http://www.etree.org/software.html](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
    
    • `md5sum /etc/passwd /etc/services > file`
  
  – Such algorithms are subject to cryptographic attack.
  
  – Therefore it is important to provide some redundancy.
How to maintain authenticity of the evidence?

• Some software, e.g. 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.