Incident Response and Forensics

Yiman Jiang, President and Principle Consultant
Sumus Technology Ltd.

James Crooks, Manager - Advisory Services

PricewaterhouseCoopers LLP

UBC 2007-04-12

Outline

- Computer Forensic Principles
- Incident Response
- Recommended Practice

Disclaimer

- Many thorny legal issues
- Consult legal counsel as necessary BEFORE using tools / techniques

We are NOT lawyers.

Newsreel

- TXJ (TJ Max, Winners. etc.) admits to losing credit + debit cards Jan 2007, the attack was discovered in Dec 2006 but not disclosed. Further disclosures indicated the attackers were in TXJ systems for an extended period. April 2007 TXJ admits over 45 million cards were stolen.
- Julie Amero (Connecticut substitute teacher) may get 40 years for exposing kid to porn in a classroom (a victim of flawed prosecution forensics and / or bad legal work)
- Utah man sentenced to 24 months in prison for bringing down wireless Internet services (December 2006)
- California man sentenced for recklessly damaging a protected computer owned by his former employer. (October 2006)

What is Computer Forensics

- Computer forensics is the collection, preservation, analysis, and presentation of computer evidence related to an incident that may or may not be a “crime”.
- Live data capture using system commands
- Capture disk / other media images (system, open source and commercial tools)
- Offline analysis
- Document entire process (significant effort)

Rules of Evidence

- Digital evidence is like any other evidence, it must follow the rules of evidence,
  - → ***Admissible***: It must conform to certain legal rules before it can be put before a court.
  - → ***Authentic***: It must be possible to positively tie evidentiary material to the incident.
  - → ***Complete***: It must tell the whole story and not just a particular perspective.
  - → ***Reliable***: There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity.
  - → ***Believable***: It must be readily believable and understandable by a court.

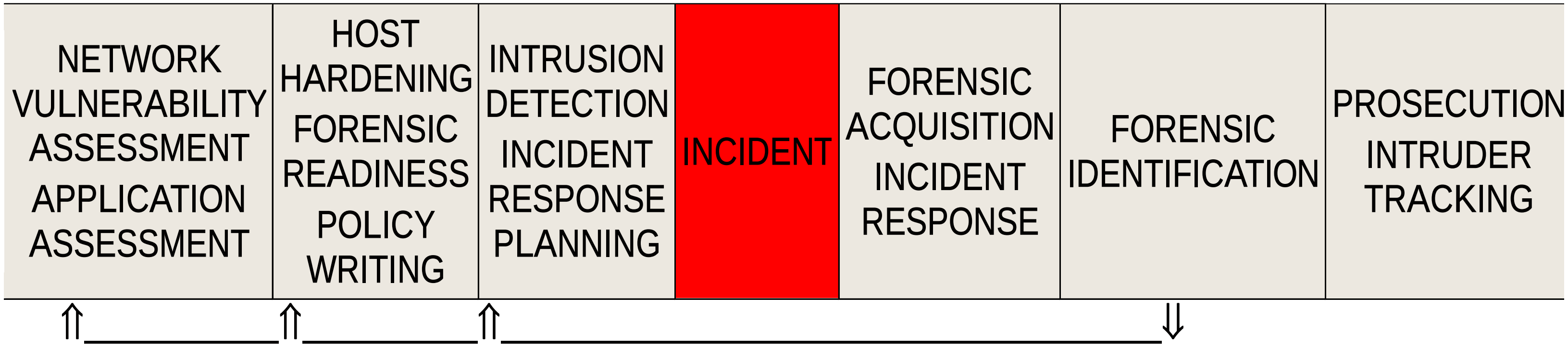
Computer Forensic Principles

- No different than non-computer forensics
- Collect and preserve "evidence" without altering or damaging original
- Authenticate that copy is identical to original
- Maintain chain-of-custody
- Perform analysis of data (without modifying it)
- Documentation of findings

Volatility of Digital Evidence

- Digital evidence is fragile and can easily be altered and destroyed through normal operation of the computer, networks, software, malware
- Order of Volatility
  - → CPU cache and register content (no forensic value)
  - → routing table, arp cache, process table, kernel statistics
  - → memory
  - → temporary file systems / swap space
  - → disk
  - → remote logging and monitoring data
  - → archival media

Lifecycle of Incident Response



NETWORK VULNERABILITY ASSESSMENT
APPLICATION ASSESSMENT

HOST HARDENING
FORENSIC READINESS
POLICY WRITING

INTRUSION DETECTION
INCIDENT RESPONSE PLANNING

INCIDENT

FORENSIC ACQUISITION
INCIDENT RESPONSE

FORENSIC IDENTIFICATION

PROSECUTION
INTRUDER TRACKING

- An incident happens at a particular time and place
- Planning and preparedness must come before an incident happens

Adopted from @stake.

Incident Response Methodology

1. Pre-incident preparation
2. Detection of incidents
3. Initial response
4. Response strategy formulation
5. Forensic collection and investigation
6. Recovery and security measure enhancement
7. Reporting
8. Follow-up

Common Mistakes in Evidence Handling

- Inappropriately dealing with the state of the victim system
- Running commands that change the file system
- Using commands and programs on the victim systems
- Not understanding all the implications of what you are doing
- Not maintaining and documenting chain of custody
- Not having an incident response plan, appropriate tools or trained staff.

Best Practice for Evidence Handling

- Secure the scene,
- Identify all evidence,
- Preserve the state the suspect computer,
- Document the hardware configuration of the system,
- Make bit-level copies of hard drives, floppy disks,
- Mathematically authenticate data on all storage devices
- Document the system BIOS date and time,
- Transport the computer system to a secure location

Two Primary Modes of Investigations

- Live Response
  - → Performed on the victim systems or relevant systems while they are live and running
- Offline Analysis
  - → Victim systems or relevant systems have been turned off, official forensic copy for record and working copy or copies made for analysis

When and Why Live Response?

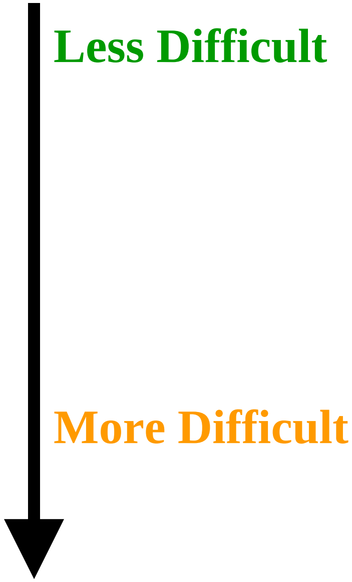
- To collect volatile information
  - → Volatile information: active information temporarily reflecting the machine’s current state, which will disappear completely upon system shutdown
- To collect information on systems that cannot be turned off

Best Practice for Collecting Volatile Information

- Determine live response strategy (if / what / how)
- Create toolkit on CD containing tested tool collections
- Avoid tools that use a GUI interface. Command line tools are best here – minimize impact
- Perform as few operations as possible
- Document all commands performed
- Capture info best way (e.g. netcat/cryptcat, floppy)
- Copy all memory
- Copy all disk (if system can’t go down)

Offline Analysis

- ➢ Using a forensic workstation, mount a working copy of the duplicated image drive in read-only mode
- ➢ Areas to search for evidence
  - → Logical File System
    - Complete, undeleted files
  - → Unallocated (free) space
    - Complete deleted files & file fragments
  - → Slack space
  - → File fragments
  - → Swap space: file fragments, working memory, passwords



Forensic Analysis – Details

1. Initial low-level analysis
2. Obtaining Modification, Access and Creation (MAC) times of all files
3. Review all pertinent logs
4. Perform keyword searches
5. Review relevant files (Application /Email messages)
6. Identify unauthorized user accounts or groups
7. Identify rogue processes / Trojans
8. Look for unusual or hidden files

Forensic Analysis – Details

Cont’d

9. Check for unauthorized access applications / non-standard ports
10. Examine pre-scheduled jobs
11. Analyze trust relationships
12. Review Security ACLs

Conclusion

- Practical investigations tend to rely on multiple sets of evidence which corroborate each other
  - → each evidence set may have its weaknesses, but taken together may point to a single conclusion
- Disk forensics may remain for some time the single most important form of digital evidence

Questions ?

Yiman Jiang

Sumus Technology Ltd. (www.sumusltd.com)
Tel: 604-838-7088
Email: yjiang@sumusltd.com

James Crooks

PricewaterhouseCoopers LLP (www.pwc.com)
Tel. 604-806-7027
Email: james.crooks@ca.pwc.com

A Series of Forensic Courses

- BCIT FSCT 8570 13 week credit course
- Yiman and James are planning to offer a series of ***one-day, hands-on*** forensic courses, sponsored by CIPS Vancouver Security SIG
  - → Course #1: Computer Forensic Principles and Data Acquisition
  - → Course #2: Investigating Windows
  - → Course #3: Investigating *NIX
  - → Course #4: Advanced Topics (Network Forensics, Data Hiding, Encryption, E-mail, etc.)