Lecture notes for digital forensics

Forensics

- Retrieval of data and artifacts from storage media
  - Generally, disk analysis & memory analysis
- Determine how an attack entered an infected system
- Analysis of computer system used as part of a crime
  - Preservation of evidence
  - Analysis must satisfy accepted legal standards

Data collection

- Sources: disks, memory dumps, USB memory sticks, cell phones
- Create bit-for-bit identical digital copy, analyze the copy
  - For drives, duplicate sector data, not filesystem data
  - Old data may remain in unused sectors
- Compute a cryptohash to later show that no changes made
- Use industry-standard analysis tools, like EnCase
- Dead analysis: stored state when powered down
- Live analysis: extract state while still running
  - Crypto keys in memory
  - RAM will hold value for short time after power loss
    - Length increases as temperature decreases (get below -60C)
  - Difficulty: live state is always changing; what is its legal standing?

File analysis

- File formats often hold metadata or hidden data
  - PDF: text hidden under redaction boxes still retrievable (demos)
  - Word: extensive undo information stored with file
    - Short text file is tens of KB long... something interesting is there
  - JPG: EXIF data (even includes GPS location)
- Log files
  - Filesystem logs
  - Web browser logs
  - Temp files (often created by a web browser)
  - Example: Audrey Seiler kidnapping
    - http://www.foxnews.com/story/0,2933,115817,00.html

    - http://www.foxnews.com/story/0,2933,115959,00.html
    - http://www.foxnews.com/story/0,2933,117088,00.html

Disk analysis

- File deletion usually doesn't... just marks blocks as available
- Journals store data copy (like 2 phase commit of databases)
- Magnetic force microscope may reveal previous magnetic states
- Bad blocks / sectors not accessible to OS-level sanitizers

Memory analysis

- Memory dumps show in-core state at time of dump
  - Even critical data often has long lifetimes, may appear in dump
  - Search for passwords, keys, kernel data structures
    - Signature matching
- Data remanence in volatile RAM
  - DRAM data retention seconds to minutes at room temperature, days when cooled by liquid nitrogen
  - To defend: power down systems when away... sleep state is insufficient

Challenges

- Mutability (booting a file system changes it)
- Encryption / stego
- Lack of qualified experts
- Maintaining chain of custody
  - Is evidence authentic?
  - Can law enforcement officers prove that they did not manipulate evidence?

Anti-forensics

- Disk sanitization: multiple overwrite with varying patterns
- Degaussing (for magnetic, not optical disks)
- Physical destruction
- Tamper-proof memory
- Immersion in solvent
- Manipulation of time & date