

## Incident Handling

### Week2: Computing & Network Basics for Forensics

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

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

1

## Road Map

- How computers work?
- How data is represented in computers?
- How networks function?
- What are the possible sources of digital evidence on the internet?
- How forensic investigations are done? What are their objectives?

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

2

## How Computers Work?

- Computer Components
- What happens when you turn the computer on?
- What is a File System?
- How is data stored on disks?
- How data is represented in computers and how it can be looked at?
- How is data in windows 2000 encrypted?

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

3

## Components of computers

- Central Processing Unit (CPU)
- Basic Input and Output System (BIOS)
- Memory
- Peripherals (disks, printers, scanners, etc)

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

4

## Boot Sequence

- What happens when you turn the computer on?
    - CPU reset: when turned on, CPU is reset and BIOS is activated
    - Power-On Self Test (POST) performed by BIOS:
      - Verify integrity of CPU and POST
      - Verify that all components functioning properly
      - Report if there is a problem (beeps)
      - Instruct CPU to start boot sequence
- (System configuration & data/time information is stored in CMOS when the computer is off. POST results compared with CMOS to report problems)

April 13, 2004

Incident Handling (G. Berg & J. Gangoly)

5

## Boot Sequence

- Disk boot: Loading of the operating system from disk into memory. The bootstrap is in Read-Only-Memory.
- **IMPORTANT POINTS**
  - CMOS chip contains important evidence on the configuration. If the battery powering CMOS is down, important evidence may be lost (Moussaoui case, 2003)
  - If the computer is rebooted, the data on the hard disk may be altered (for example the time stamps on files).
  - Hence the importance of booting from a floppy and accessing the CMOS setup during the boot up.

April 13, 2004

Incident Handling (G. Berg & J. Gangoly)

6

## Boot Sequence: Important Points

- It is a good idea to obtain BIOS password from user. Resetting CMOS password can change system settings and hence alter evidence. For example, you can change the boot sequence so that the computer accesses drive A first.
- It is possible to overwrite BIOS passwords using services such as [www.nortek.on.ca](http://www.nortek.on.ca). However, one should use it as a last resort
- It may be necessary to physically remove the hard disk to retrieve data

April 13, 2004

Incident Handling (G. Berg & J. Gangoly)

7

## The File System

- File system is like a database that tells the operating system where is what data on the disks or other storage devices.
  - FAT in MS-DOS is a flat table that provides links to their location on disks. But Microsoft's NTFS is similar to unix file systems.
  - In unix systems, it consists of a (inode) table providing pointers from file identifiers to the blocks where they are stored, and a directory.

April 13, 2004

Incident Handling (G. Berg & J. Gangoly)

8

## The File System

- Mounting a file system is the process of making the operating system aware of its existence. When mounted, the operating system copies the file tables into kernel memory
- The first sector in a hard disk contains the master boot record which contains a partition table. The partition table tells the operating system how the disk is divided
- Partitions can be created and viewed using **fdisk**. Each partition contains the boot sector, primary and secondary file allocation tables (FAT), the root directory, and unallocated space for storing files.
- Formatting a partition (using **format** in windows or **mkfs** in unix) "prepares" it for recognition by the operating system as a file system.

April 13, 2004

Incident Handling (G. Berg & J. Gangoly)

9

## The File System: Important Points

- Formatting a hard drive does not erase data, and therefore the data can be recovered
- Low-level formatting does erase data. However, special vendor software is needed to low-level format hard disks

April 13, 2004

Incident Handling (G. Berg & J. Gangoly)

10

## Disk Storage

- Data is stored on the disk over concentric circles called *tracks* (heads). When the disks are stacked, the set of tracks with identical radius collectively are called a *cylinder*. The disk is also divided into wedge-shaped areas called *sectors*.
- Disk capacity is given by the product of number of cylinders, tracks, and sectors. Each sector usually stores 512 bytes.

April 13, 2004

Incident Handling (G. Berg & J. Gangoly)

11

## Disk Storage

- Zoned Bit Recording (ZBR) is used by disk manufacturers to ensure that all tracks are all the same size. Otherwise the inner tracks will hold less data than the outer tracks.

April 13, 2004

Incident Handling (G. Berg & J. Gangoly)

12

## Disk Storage

- The tracks on disks may be one of
  - Boot track (containing partition and boot information)
  - Tracks containing files
  - Slack space (unused parts of blocks/clusters)
  - Unused partition (if the disk is partitioned)
  - Unallocated blocks (usually containing data that has been “deleted”)

(When the program execution is complete, the allocated memory reverts to the operating systems. Such unallocated memory is not physically erased, just the pointers to it is deleted)

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

13

## Disk Storage: Important Points

- Hard drives are difficult to erase completely. Traces of magnetism can remain. This is often an advantage, since evidence may not have been erased completely by the perpetrator. Such evidence can be recovered using one of the data recovery services (such as [www.ontrack.com](http://www.ontrack.com), [www.datarecovery.net](http://www.datarecovery.net), [www.actionfront.com](http://www.actionfront.com), [www.ibas.net](http://www.ibas.net) )
- Files “deleted” may be partially recovered since their fragments may still be in unallocated blocks

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

14

## Disk Storage: Important Points

- Traces of information can remain on storage media such as disks even after deletion. This is called *remanence*. With sophisticated laboratory equipment, it is often possible to reconstruct the information. Therefore, it is important to preserve evidence after an incident.
- A perpetrator can hide data in the inter-partition gaps (space between partitions that are specified while partitioning the disk) and then use disk editing utilities to edit the disk partition table to hide them.

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

15

## Disk Storage: Important Points

- The perpetrator can hide data in NT Streams, and such streams can contain executables. They are NOT visible through windows explorer and can not be seen through any GUI based editors (This week’s assignment)
- The perpetrator can declare smaller than actual drive size while partitioning and then save information at the end of the drive.
- Many of the above can be uncovered by using disk editors such as winhex, Hex Workshop, or Norton Disk Editor if the disks are formatted for one of the Microsoft operating systems.

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

16

## Disk Storage: Important Points

- For linux systems, LDE (Linux Disk Editor at [lde.sourceforge.net](http://lde.sourceforge.net)) is a similar utility available under Gnu license.
- **Main Lesson: Do not depend on directories or windows explorer. Get to the physical data stored on the disk drives. Do not look only at the partitioned disk. Incriminating data may be lurking elsewhere on the disk.**

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

17

## Data Representation

- While all data is represented ultimately in binary form (ones and zeroes), use of editors that provide hexadecimal or ascii format display of data are valuable in forensics. They allow you to see features that are otherwise not visible.
- Popular tools for viewing such files include Winhex ([www.winhex.com](http://www.winhex.com)), Hex Workshop ([www.hexworkshop.com](http://www.hexworkshop.com)), and Norton Disk Edit ([www.symantec.com](http://www.symantec.com))

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

18

## Data Representation: Important point

- **One should be careful in using such editors, since data can be destroyed inadvertently.**

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

19

## Encryption

- With Windows 2000, Microsoft introduced NTFS Encrypted File System (EFS) using asymmetric keys: the operating system holds the public key while the owner of the data holds the private key.
- The windows 2000 operating system automatically sends a recovery certificate (containing the recovery key) to the account of the server administrator or the administrator of the standalone machine.

April 13, 2004

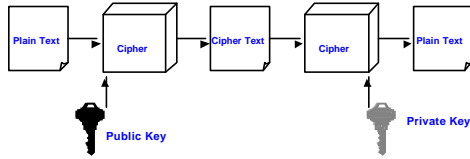
Incident Handling (G. Berg & J. Gangolly)

20

## Asymmetric Encryption

(Source: <http://www.albany.edu/~goel/classes/spring2002/MS1416/cryptography.ppt>)

- Uses a pair of keys for encryption
  - Public key for encryption
  - Private key for decryption
- Messages encoded using public key can only be decoded by the private key
  - Secret transmission of key for decryption is not required
  - Every entity can generate a key pair and release its public key



April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

21

## Computer Networks

- How are internet communications organised?
- How the internet protocols work?
- What are some of the vulnerabilities caused by the internet protocols?

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

22

## Networking

- The Internet Model:
  - Application Layer (http, telnet, email client,...)
  - Transport Layer: Responsible for ensuring data delivery. (Port-to-Port) (Protocols: TCP and UDP) (Envelope name: segment)
  - Network Layer: Responsible for communicating between the host and the network, and delivery of data between two nodes on network. (Machine-to-Machine) (Protocol: IP) (Envelope name: datagram) (Equipment: Router)
  - Data Link Layer: Responsible for transporting packets across each single hop of the network (Node-to-Node) (Protocol: ethernet) (Envelope name: Frame) (Equipment: Hub)
  - Physical Layer: Physical media (Repeater-to-repeater) (Equipment: Repeater)

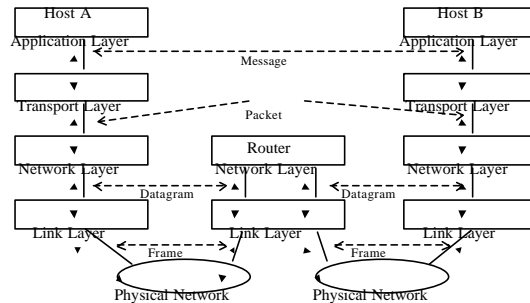
April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

23

## Protocol Layering – Routing

(Source: <http://www.albany.edu/~goel/classes/spring2002/MS1416/internet.ppt>)



April 13, 2004

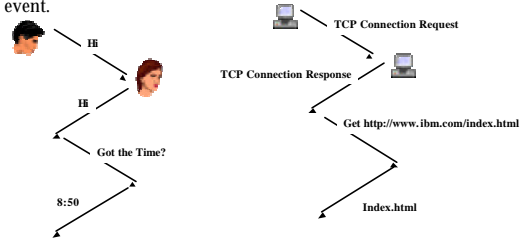
Incident Handling (G. Berg & J. Gangolly)

24

## Protocols

(Source: <http://www.albany.edu/~goel/classes/spring2002/MS1416/internet.ppt>)

A protocol defines the format and the order of messages exchanged between two or more communicating entities as well as the actions taken on the transmission and/or receipt of a message or other event.



April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

25

## Some Protocol Vulnerabilities

- **TCP** Connection Oriented Service (Establish connection prior to data exchange, coupled with reliable data transfer, flow control, congestion control etc.)
  - Port scanning using netstat (unix/windows) or Nmap (<http://www.insecure.org/nmap/>)
  - Attacker can mask port usage using kernel level Rootkits (which can lie about backdoor listeners on the ports)
  - Attacker can violate 3-way handshake, by sending a RESET packet as soon as SYN-ACK packet is received

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

26

## Some Protocol Vulnerabilities

- **UDP** Connectionless Service (No handshake prior to data exchange, No acknowledgement of data received, no flow/congestion control)
  - Lack of a 3-way handshake
  - Lack of control bits hinders control
  - Lack of packet sequence numbers hinders control
  - Scanning UDP ports is also harder, since there are no code bits (SYN, ACK, RESET). False positives are common since the target systems may not send reliable "port unreachable" messages

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

27

## Sources of evidence on the internet?

- Evidence can reside on the computers, network equipment (routers, for example), and on servers
- Various tools are available to extract evidence from these sources

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

28

## Evidence on workstations & Servers

- Locations (Disks)
  - Disk partitions, inter-partition gaps (not all partitions may have file systems. For example, swap space in unix systems do not have file systems)
  - Master Boot Record (contains partition table)
  - Boot sector (has file system information)
  - File Allocation Tables (FAT)
  - Volume slack (space between end of file system and end of the partition)
  - File slack (space allocated for files but not used)
  - RAM slack (in case of pre windows 95a, space between end-of-file and end-of-sector)

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

29

## Evidence on workstations, Servers

- Locations (continued)
  - Unallocated space (space not yet allocated to files. Also includes recently deleted files, some of which might have been partially overwritten)
- Locations (Memory or RAM)
  - Registers & Cache (usually not possible to capture. Cache can be captured as part of system memory image)
  - RAM
  - Swap space (on disk)

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

30

## Evidence on Servers & Network Equipment

- Router systems logs
- Firewall logs of successful and unsuccessful attempts
- Syslogs in /var/logs for unix systems
- wtmp logs (accessed with last command) in unix systems

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

31

## Evidence on Workstations, Servers, Network: Important Points

- **It is possible to hide partitions**
- **It is possible to hide data in files using streams so they are not visible. You can know of their existence only by analyzing the Master File Table**
- **It is possible to hide data in inter-partition gaps, volume slack**
- **It is possible to hide data at the end of the drive by declaring drive size smaller than its actual size.**

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

32

## How to obtain admissible evidence?

- The Forensic Investigation Process
  - Incident alert or accusation: violation of policy or report of crime
  - Assessment of worth/damage: To set priorities
  - Incident/Crime scene protocols: Actions taken at the scene
  - Identification and seizure of evidence: Recognition of evidence and its proper packaging (protection)
  - Preservation of evidence: Preserve the integrity of the evidence obtained

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

33

## The Forensic Investigation Process

- Recovery of evidence: recovery of hidden and deleted information, recovery of evidence from damaged equipment
- Harvesting: Obtaining data about data
- Data reduction: Eliminate/filter evidence
- Organization and search: Focus on arguments
- Analysis: Analysis of evidence to support positions
- Reporting: Record of the investigation
- Persuasion and testimony: In the courts

(Source: *Digital Evidence & Computer Crime*, Eoghan Casey, Elsevier, 2004)

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

34

## Objectives of the Investigative Process

- Acceptance: Process has wide acceptance
- Reliability: Methods used can be trusted to support findings
- Repeatability: Process can be replicated
- Integrity: Trust that the evidence has not been altered
- Cause & Effect: Logical relationship between suspects, events, evidence
- Documentation: Recording of evidence

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

35

## Synopsis

- How computers work?
- How data is represented in computers?
- How networks function?
- What are the possible sources of digital evidence on the internet?
- How forensic investigations are done? What are their objectives?

April 13, 2004

Incident Handling (G. Berg & J. Gangolly)

36