

Incident Handling

State University of New York at Albany

4/4/2004

Incident Handling Week 1 (J Gangolly)

1

Incident Handling

- The Roadmap
 - **April 6, 2004:** What is an incident, what are various types of incidents
 - **April 13, 2004:** Computing/Forensic Background
 - **April 20, 2004:** Live Computer Forensics (Frank Adelstein)
 - **April 27, 2004:** Legal aspects of evidence, reporting incidents. How to prevent, detect, and handle incidents. What are various types of evidence.
 - **May 4, 2004:** How to handle evidence: Preserve, protect, and maintain chain of custody (Computer Forensics). Incident Response Planning

4/4/2004

Incident Handling Week 1 (J Gangolly)

2

Incident Handling - Week 1

- What is an Incident? How does it differ from any other event?
- What are the different types of incidents? How do they happen, and how they affect systems?
- What are the sources of information about incidents?
- How to use such information to learn about incidents?

4/4/2004

Incident Handling Week 1 (J Gangolly)

3

Events and Incidents

- An event is *any occurrence in a computerised information system that can be observed*. On the other hand, incidents are adverse events with negative consequences that are security related.
- Events are usually logged by the operating systems, but all incidents may not be logged automatically. You will need to go beyond the logs to study an incident. For example, an incident may consist of a pattern of events.
- Logs provide clues that help study incidents

4/4/2004

Incident Handling Week 1 (J Gangolly)

4

Events

- Events logged by the operating system can be viewed.
- For example,
 - **MS-windows-2000:**
they can be viewed in MS-windows-2000 systems by
Start -> Settings -> Control Panel -> Administrative Tools -> Event Viewer.
The three main event logs in windows-2000 are AppEvent.Evt, SecEvent.Evt, and SysEvent.Evt. They can be found in the directory `\WinNT\SYSTEM32\CONFIG`
 - **Unix systems:**
/etc/wtmp contains information about operations, in addition to logs of the unix accounting system. *ps -aux* is also helpful.

4/4/2004

Incident Handling Week 1 (J Gangolly)

5

Incidents

- Incidents are
 - adverse events (they are not usual)
 - with negative consequences (they impose costs/burdens) that are
 - perpetrated by persons (either directly or through programs) with a
 - malicious intent to harm (usually the perpetrator means to cause harm).

4/4/2004

Incident Handling Week 1 (J Gangolly)

6

Events vs. Incidents

- Events caused by nature are not considered incidents for the purpose of this course, even though they have adverse consequences for organisations. **This difference is crucial. An organisation must protect itself against events as well as incidents, but we will consider only incidents.**
- Incidents may not always impose costs (for example, distribution of pornography or merely violating one's privacy)

4/4/2004

Incident Handling Week 1 (J Gangolli)

7

Incidents

- Sometimes, the adverse events are caused deliberately (or occasionally without any malicious motive) to breach *confidentiality*, compromise *integrity*, or degrade *availability* of computerised systems.
 - *confidentiality* of a computerised information systems is breached when an unauthorised person gains access to a resource (system, files, equipment, etc)
- **Examples:**
 - Unauthorised person logging to the system
 - Unauthorised person views or copies a file

4/4/2004

Incident Handling Week 1 (J Gangolli)

8

Incidents

– *integrity* of computerised information systems is compromised by unauthorised alteration of the information in it

- **Examples:**
 - An unauthorised user deletes a record from a database
 - An unauthorised user changes some text in a file
 - An unauthorised user copies some information from one file to another
 - An unauthorised user changes some statements in a program
 - An unauthorised user executes a program

4/4/2004

Incident Handling Week 1 (J Gangolli)

9

Incidents

– *availability* of the computerised information systems is degraded when it is not able to provide access or resources to authorised users

- **Examples:**
 - Customers are not able to access an e-Commerce website because of a Denial-of-Service attack
 - Authorised users are unable to use the system because the system has been brought down by the perpetrator

4/4/2004

Incident Handling Week 1 (J Gangolli)

10

Incidents

- Incidents usually involve
 - Breach of security policies of the organisation
 - Perpetrators with a malicious intent to harm
 - Involve inappropriate use of the organisation resources by unauthorised persons
 - Preventing the use of the computer resources by authorised users and applications

4/4/2004

Incident Handling Week 1 (J Gangolli)

11

Importance of Security Policies

- If an organisation does not have security policies, it is difficult to say if an incident has occurred. **For example, if access control policies don't exist, how to detect insider caused incidents?**
- While some events are obviously incidents, it is a good idea to know precisely when an event can be classified as an incident. Security policies are crucial for this.

4/4/2004

Incident Handling Week 1 (J Gangolli)

12

Malicious Intent and Incidents

- Incidents can be perpetrated by those simply seeking the thrill, and those who mean to cause harm.
- The latter are significantly more dangerous, since they can penetrate and cause further harm even after an incident has been detected. They will seek alternative means of entry (they may already have set up backdoors for such entry).

4/4/2004

Incident Handling Week 1 (J Gangolly)

13

Inappropriate use of Resources

- Incidents usually involve inappropriate use of resources by an unauthorised party.
 - Use of stolen passwords,
 - use of computing resources to launch denial-of-service attacks on other systems,
 - use such resources to distribute illegal materials (pornography, for example),
 - to violate law by illegal distribution/dissemination of information (for example, violation of export regulations)

4/4/2004

Incident Handling Week 1 (J Gangolly)

14

Prevention of Resource use

- Most large organisations have become dependent on information systems for their very existence, and consequently they have become mission critical. **Jeopardizing the availability of such systems can cause mass disruption of business.**

4/4/2004

Incident Handling Week 1 (J Gangolly)

15

Incidents– Why difficult to detect

- Incidents are often very difficult to detect because:
 - The intruder may not leave a trace or footprints
 - The intruder may not have altered any data and therefore it is not known if there has been an incident
 - An insider may be responsible for it, and therefore not raise any suspicion, thus preventing detection
 - The volume of event log data is so voluminous that it is difficult to detect
 - The intruder may “fly low” to avoid detection

4/4/2004

Incident Handling Week 1 (J Gangolly)

16

Lack of Perpetrator's Footprints

- Often, a perpetrator may not leave any footprints, and even if there are footprints, they may be normal and therefore not raise suspicion
 - For example, a perpetrator may have gained entry by using a stolen or cracked password.
Suspicious are not raised because, on the surface, it is an authorised user who entered the system
 - For example, the entry may have been through compromise of root or administrative password, and therefore **logs may not be reliable.**

4/4/2004

Incident Handling Week 1 (J Gangolly)

17

Data Not Altered

- The perpetrator may not have altered the data but just read it.
 - **Mere violation of confidentiality of data alters the meaning of data**
 - **It is easy to reproduce such data without incurring significant costs**
 - **In electronic systems, the only protection that data has are measures that have been engineered in the design (for example access controls in operating systems and Database management systems)**

4/4/2004

Incident Handling Week 1 (J Gangolly)

18

Incidents caused by Insiders

- Evidence suggests that a majority of incidents are caused internally. Examples include
 - Insiders who have access to information resources executing unauthorised transactions
 - Distribution of pornography
 - Introduction of viruses through floppy disks
 - Denial of service attacks on external systems launched from within the network
 - Insiders altering or hiding data

4/4/2004

Incident Handling Week 1 (J Gangoly)

19

Avoiding detection

- Data on network traffic is so voluminous that databases for intrusion detection systems have a narrow window. This fact is exploited by hackers to avoid detection.
 - For example, they can straddle windows by slowing data transmission rate, or revisiting sites in different windows

4/4/2004

Incident Handling Week 1 (J Gangoly)

20

Incidents

- “.. violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.”

Source: *DRAFT Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, Tim Grance, Karen Kent, Brian Kim

4/4/2004

Incident Handling Week 1 (J Gangoly)

21

Incidents

- It is important to have policies on acceptable use and security. **Otherwise an incident is not even properly defined**
- It is important to have standard security practices so that the risk of incidents is minimised.

4/4/2004

Incident Handling Week 1 (J Gangoly)

22

Threats and Vulnerabilities

- A **threat** is the potential cause of an unwanted event that may result in harm to the agency and its assets.
- **Vulnerability:** A characteristic (including a weakness) of an information asset or group of information assets which can be exploited by a threat.

Source:
(<http://www.oit.nsw.gov.au/pdf/4.4.16.IS1.pdf>)

4/4/2004

Incident Handling Week 1 (J Gangoly)

23

Threats and Vulnerabilities

- Threats exploit vulnerabilities in order to cause harm (theft, destruction, corruption, modification, and/or disclosure of data/assets, misuse of resources, interruption of services).
 - **An incident is the realisation of a threat;**
 - **a threat is the manifestation of vulnerabilities;**
 - **vulnerabilities are consequences of weaknesses in controls over assets and data.**

4/4/2004

Incident Handling Week 1 (J Gangoly)

24

Threats and Vulnerabilities

- Destruction (facilities, data, equipment, communications, personnel);
- Corruption or modification (data, applications);
- Theft, removal or loss (equipment, data, applications);
- Disclosure (data);
- Use or acceptance (unlicensed software, repudiated or false data);
- Interruption of services.

4/4/2004

Incident Handling Week 1 (J Gangoly)

25

Vulnerabilities

- Since vulnerabilities are usually the root cause of incidents, it is important to have a good understanding of
 - Types of vulnerabilities
 - Possible sources of attacks
 - The Information systems components that are vulnerable
 - The types of losses that can be sustained
 - The software types that are subject to the vulnerabilities

4/4/2004

Incident Handling Week 1 (J Gangoly)

26

Vulnerabilities

- Need for common naming of vulnerabilities and exposures
 - Common Vulnerabilities & Exposures (CVE effort www.mitre.org)
 - CVE Version 20030402
- Need for a Vulnerabilities Database
 - ICAT Database at www.nist.gov

4/4/2004

Incident Handling Week 1 (J Gangoly)

27

Vulnerabilities

- Need for architecting Incident Response in organisations
 - *Handbook for Computer Security Incident Response Teams (CSIRTs)* CMU/SEI
 - *DRAFT Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology (NIST)*

4/4/2004

Incident Handling Week 1 (J Gangoly)

28

Types of Vulnerabilities

- Input validation errors
 - Boundary Overflow
 - Buffer overflow
 - Access validation error: **Faulty access control mechanism**
 - Exceptional condition handling error
 - Environmental error: **Configuration of user controllable settings make the system vulnerable**
 - Configuration error
 - Race condition: **A device tries to perform two or more operations at the same time**
 - Design error
- (Source: http://icat.nist.gov/icat_documentation.htm)

4/4/2004

Incident Handling Week 1 (J Gangoly)

29

Exposed Environment Component

- Operating system
 - Server application
 - Non-server application
 - Communication protocol
 - Encryption module
 - Hardware
 - Other
- (Source: www.icat.nist.gov)

4/4/2004

Incident Handling Week 1 (J Gangoly)

30

Incidents and Crimes

- The forensic principles we study here apply to incidents as well as crimes
- Computer crimes under **US Comp. Fraud & Abuse Act**
 - Theft of computer services
 - Accessing computers without authorisation
 - Theft or alteration of electronically stored information
 - Extortion committed with the assistance of computers
 - Unauthorised access to information at financial institutions, credit card companies, credit reporting agencies
 - Traffic in stolen passwords
 - Transmission of viruses, etc.

4/4/2004

Incident Handling Week 1 (J Gangolly)

31

Types of Cybercrime (Parker, 1998)

- Computer is the object of crime
 - Stealing or destroying a computer
- Computer is the subject of crime
 - Infecting a computer with a worm or virus
- Computer used as a tool in committing crime
 - Running programs on a computer to perpetrate a crime, eg., distribution of pornography
- Computer as a symbol is used to commit crime
 - Scaring people into paying for nonexistent services

4/4/2004

Incident Handling Week 1 (J Gangolly)

32

Types of Cybercrime (Parker, 1998)

- In each of the above types of crimes, the computer has valuable evidence that needs to be collected and protected.
 - Extraction of data from a damaged computer
 - Obtaining data from an infected computer
 - Obtaining evidence from a computer that was used in committing the crime

References:

Digital Evidence/Computer Crime: Forensic Science, Computers and the Internet, Eoghan Casey, (Academic Press, 2000)

Fighting Computer Crime: A New Framework for Protecting Information, D. Parker, (John Wiley, 1998)

4/4/2004

Incident Handling Week 1 (J Gangolly)

33

Types of Cybercrime (Carter, 1995)

- Computer is the target of crime
 - Intrusion/Trespass, Theft, vandalism, DoS attack,...
- Computer is used in committing the crime
 - Credit card fraud, telecommunications fraud,...
- Coincidental use of computers in committing crime
 - Use of computers in pornography, drug dealing, money laundering,...

References:

"Computer Crime Categories", D.L. Carter, FBI Law Enforcement Bulletin, July 1995)

4/4/2004

Incident Handling Week 1 (J Gangolly)

34

Threats, Vulnerabilities, and Information Security

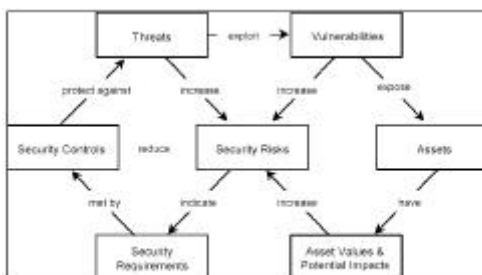


Figure 3: Risk concept relationship

(Source: Australian Standard Handbook of Information Security Risk Management – HB231:2000)

4/4/2004

Incident Handling Week 1 (J Gangolly)

35

Incident related Communications

(Source: DRAFT Computer Security Incident Handling Guide: Recommendations of the NIST)



Figure 2-1. Incident-Related Communications With Outside Parties

4/4/2004

Incident Handling Week 1 (J Gangolly)

36

Incident Response Lifecycle

(Source: DRAFT Computer Security Incident Handling Guide: Recommendations of the NIST)



Figure 3-1. Incident Response Life Cycle

4/4/2004

Incident Handling Week 1 (J Gangolly)

37

Synopsis

- What is an incident and how it differs from events?
- What are the characteristics of incidents?
- What are vulnerabilities, threats, and weaknesses in controls in systems?
- What are the various vulnerabilities? How does one find information about them and their impact on incidents?
- Incidents and computer/cyber crimes
- Types of cyber crimes
- Incident Response Life Cycle

4/4/2004

Incident Handling Week 1 (J Gangolly)

38