Incident Handling

University at Albany
State University of New York
Incident Handling

• The Roadmap
  – **WEEK 1**: What is an incident, what are various types of incidents?
  – **WEEK 2**: How to prevent, detect, and handle incidents. What are various types of evidence?
  – **WEEK 3**: How to handle evidence: Preserve, protect, and maintain chain of custody (Computer Forensics)
  – **WEEK 4**: Legal aspects of evidence, reporting incidents, *etc.*, 
  – **WEEK 5**: Incidence Response Planning
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 do they affect systems?
• What are the sources of information about incidents?
• How to use such information to learn about incidents?
Events and Incidents

• An **event** is *any occurrence in a computerised information system that can be observed.*

• An **Incidents** is an adverse event with negative consequences that are security related.

• Events are usually logged by operating systems, but all incidents may not be logged automatically.
  – You may need to go beyond the logs to study an incident.
    For example, an incident may consist of a pattern of events.

• Logs provide clues to help study incidents.
Events

• Events logged by the operating system can be viewed.
Events

• For example,
  – **MS-windows-2000:**
    • They can be viewed in MS-windows-2000 systems by
      \textit{Start} -> \textit{Settings} -> \textit{Control Panel} -> \textit{Administrative Tools} -> \textit{Event Viewer}.
    • The three main event logs in windows-2000 are
      – \texttt{AppEvent.Evt},
      – \texttt{SecEvent.Evt}, and
      – \texttt{SysEvent.Evt}.
    • They can be found in the directory \texttt{\WinNT\SYSTEM32\CONFIG}
Events

• For example,
  – **Unix systems:**
    • `/etc/wtmp` contains information about operations, in addition to logs of the unix accounting system.
    • `ps -aux` is also helpful.
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).
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).
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.
Incidents

• **Confidentiality** of a computerized information systems is breached when an unauthorized person gains access to a resource (system, files, equipment, etc.)
  
  • **Examples:**
    
    – Unauthorized person logging to the system.
    – Unauthorized person views or copies a file.
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.
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.
Incidents

• Incidents usually involve
  – Breach of security policies of the organization,
  – Perpetrators with a malicious intent to harm,
  – Inappropriate use of the organisation resources by unauthorised persons,
  – Preventing the use of the computer resources by authorised users and applications.
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.
Malicious Intent and Incidents

• Incidents can be perpetrated by those simply seeking a 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).
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 the law by illegal distribution/dissemination of information (for example, violation of export regulations).
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.
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.
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.
    - Suspicions 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.
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 have are measures that have been engineered in the design
    • For example access controls in operating systems and Database management systems.
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.
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.
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.
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.
Threats and Vulnerabilities

- **Vulnerability**: a flaw in software or a system that produces an exploitable weakness.
- **Exploit**: a malicious technique deliberately targeting a system or program vulnerability.
- **Control (Mitigation)**: a measure taken to close or minimize a vulnerability.
Threats and Vulnerabilities

• A threat is the potential cause of an unwanted event that may result in harm to the agency and its assets.
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.
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 (unlicenced software, repudiated or false data);
- Interruption of services.
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.
Vulnerabilities

• Need for common naming of vulnerabilities and exposures
  – Common Vulnerabilities & Exposures (CVE) list
    • www.mitre.org
    • CVE Version 20030402

• Need for a Vulnerabilities Database
  – ICAT Database at www.nist.gov
Vulnerabilities

• Need for creating 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)
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)
Exposed Environment Components

- Operating system
- Server application
- Non-server application
- Communication protocol
- Encryption module
- Hardware
- Other

- (Source: www.icat.nist.gov)
Incidents and Crimes

• The forensic principles we study here apply to incidents as well as crimes

• Computer crimes under *US Comp. Fraud & Abuse Act* (18 USC 1030)
  – Theft of computer services,
  – Accessing computers without authorization,
  – 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.*
Types of Cybercrime (Parker, 1998)

• Computer is the *object* of a crime
  – Stealing or destroying a computer

• Computer is the *subject* of a crime
  – Infecting a computer with a worm or virus

• Computer used as a *tool* in committing a crime
  – Running programs on a computer to perpetrate a crime, *e.g.*, distribution of pornography

• Computer as a symbol is used to commit a crime
  – Scaring people into paying for nonexistent services
Types of Cybercrime (Parker, 1998)

- In each of the preceding 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:


Types of Cybercrime
(Carter, 1995)

• Computer is the target of crime
  – Intrusion/Tresspass, 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:
Threats, Vulnerabilities, and Information Security

Figure 3: Risk concept relationship
Incident Related Communications

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

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

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

Figure 3-1. Incident Response Life Cycle
Synopsis

• What is an *incident* and how it differs from an *event*?
• What are the characteristics of incidents?
• What are the 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.