Handling Security Incidents

Chapter 7

Lecturer: Pei-yih Ting

Overview

- Attacks
- Security Incidents
- Handling Security Incidents
- Incident management Methods and Tools
- Maintaining Incident Preparedness
- Standard Incident Handling Procedures
- Learn from Experience
- Malicious code
- Common Types of Attacks

Attack Terms and Concepts

- An attack is any attempt to
  - Gain unauthorized access to a system
  - Deny authorized users from accessing a system
- The purpose of an attack is to
  - Bring about data disclosure, alteration, or denial (DAD)
- An attacker is an individual (or group) who strives to violate a system's security
- When an attacker breaks a law or regulation, a computer crime occurs

Types of Attacks

- Military and Intelligence Attacks
  - Attacks are attempts to acquire secret information from military or law enforcement agencies
    - For example, defense strategies, sealed legal proceedings
    - Cause serious damage or result in great expense to change and reformulate plans
- Business Attack
  - Similar to a military attack, but the target is a commercial organization
  - Purpose is to access sensitive data
    - For example, trade secret information or important business decisions

Types of Attacks (cont'd)

- Financial Attack
  - Target is a commercial organization
  - Purpose is to acquire goods, services, or money improperly
    - For example, phone phreaking
- Terrorist Attacks
  - Coordinates with a physical attack by disrupting communication and infrastructure control systems
  - Purpose is to affect the ability of agencies to react to the physical attack

Types of Attacks (cont'd)

- Grudge Attacks
  - Purpose is to inflict damage or seek revenge against an organization
  - Former employees comprise a large number of these attackers
- Fun Attacks
  - No real purpose except bragging rights for the hacker
  - Can be very difficult to track down

Security Incidents

- A security **incident** is defined as any violation of a security policy
  - Every attack is an incident
  - Not every incident is an attack, ex. accessing Internet auction sites during office hour or using dictionary word for a password
- Incident recognition starts with user education
  - Users should know what the policies are so they will know when an incident has occurred
  - Users should also be educated about what to do if they notice that an incident has occurred
- Many incidents go unresolved because they are unnoticed

Handling Security Incidents

- First step: recognizing an incident has occurred
  - The security policy should clearly state actions and behaviors that constitute a security incident.
  - Some incidents are discovered after the fact through log analysis or system audit
    - For example, unauthorized access to secure files discovered by scanning an access log
  - Some incidents are identified and examined as they occur
    - DOS attacks are usually apparent as they occur
- Second step: There are four general types of incidents. Each type of incidents presents its own challenges in detection and avoidance.

Handling Security Incidents (cont'd)

Four types of security incidents:

- Scanning
  - The systematic probing of ports to find open ports and query them for information
  - Not an attack, but may be a precursor to an attack
  - Looking for packet traces in the log file of a firewall
- Compromise
  - Any unauthorized access to a system
  - Generally involves defeating or bypassing security controls
  - Detecting compromise is difficult, usually by noticing something unusual in system activities

Handling Security Incidents (cont'd)

- Malicious code
  - Any program, procedure, or executable file that makes unauthorized modifications or triggers unauthorized activities
  - Viruses, worms, Trojan horses fall into this category
  - Noticing strange behaviors of your system
  - Antivirus S/W catches these by signature matching
- Denial of Service (DoS)
  - Violates the availability property of security
  - Denies authorized users access to a system
  - Highly disruptive to online retailers (business platform on the Internet)
  - Denies the attacker's IP

Incident Management Methods

- A security policy should have incident handling plans for all probable incidents
- General procedures
  - Detect that an incident has occurred
  - Contain the damage caused by the incident
  - Assess the damage and report the incident
  - Investigate the origin of the incident
  - Collect evidences
  - Analyze findings
  - Take action to avoid another occurrence
  - Recover from the damage

Incident Management (cont'd)

- Often a standing **incident response team** is created with members from different departments within an organization
- IRT ensures that an incident is handled efficiently
- IRT collects information from an attack for analysis (promote any changes that will reduce the likelihood of a reoccurrence) and possible legal action
- IRT investigates an incident by collecting evidence that can be used to verify the identity or activity of an attacker

Incident Management (cont'd)

- The analysis of a system to find evidence of attack activity is called system forensics
- Tools used to collect evidence include
  - Log file analyzers, disk search and scanning tools, network activity tracing tools
- When an incident occurs, a rule of thumb is to call law enforcement officials in immediately if you think there is any chance a violation of the law has occurred

Maintain Incident Preparedness

- An incident response team should be prepared for all viable incidents
  - When forming an incident response team, take advantage of resources that provide additional information and guidance on how teams operate
- The incident response team should be trained to follow security policy procedures
  - Each team member should know his/her own role and possibly other roles as well
- Establish a relationship with law enforcement officials who may be called in when incidents occur
- Users should know how to recognize common incidents and what to do if they notice one

Maintain Incident Preparedness (cont'd)

Table 7.1 Incident Response Team Resources

Resource	URL
Handbook for Computer Security Incident Response Teams	http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf
Computer Security Incident Response Team	http://www.cert.org/csirts
Responding to Intrusions	http://www.cert.org/security-improvement/modules/m06.html
Forming an Incident Response Team	http://www.auscert.org.au/render.html?it=2252&cid=1920
SANS IESEC Reading Room: Incident Handling	http://www.sans.org/rr/catindex.php?cat_id=27
FIRST: Forum of Incident Response and Security Teams	http://www.first.org/

Using Standard Incident Handling Procedures

- When an incident response team is mobilized, they should follow written procedures from the security policy
- Each team member should fill out a standard incident report
  - It is important to maintain a document trail throughout
- Make sure that your procedures will meet any requirements for law enforcement

Postmortem: Learn from Experience

- After an incident, complete any research or documentation and review the handling process
- The response team should meet as quickly as possible to debrief
  - Review the incident and consider why and how it happened, can it happen again, what changes might be good
  - Review team performance and consider what went well, what did not, what changes might be useful to make the team more effective
- Encourage all team members to research what other organization have published on the topic of incident response

Malicious Code

- Best defense against malicious code is a good offense
  - Use shields such as virus scanners
  - Use intrusion detection system (IDS)
- Be careful about executable files that are introduced into your system
  - Any data entry point into a system can be used to introduce malicious code including floppy disks, data ports, networks, and removable storage devices
  - Viruses can be detected using several techniques including signature scans, changed size or time-date stamps, cryptographic hashes, and digital signatures
  - Active-X controls or Java native code executed in a browser is dangerous

Malicious Code (cont'd)

- Viruses
  - A program that embeds a copy of itself inside of an executable file and attempts to perform unauthorized data access or modification
  - A virus needs a host software in order to run
- Worms
  - A standalone program that tries to perform some type of unauthorized data access or modification
- Logic Bombs
  - Executes a sequence of instructions when a specific system event occurs
  - Usually hides itself as a virus in system executables

About Malicious Code (cont'd)

- Trojan horses
  - Similar to a worm
  - Appears to have some useful or neutral purpose
  - Performs some malicious act when run
- Active Content Issues
  - The Internet is one of the most common entry points for malicious code
  - Downloadable plug-ins perform many useful functions but make it easy to send malicious code
  - Java sandbox model
  - Active X control (digitally signed)

Common Types of Attacks

- Back Doors
  - Programmers often leave an "opening" in software they write to allow them to gain entrance without going through normal security control
  - Once discovered, these openings can be exploited by anyone
- Brute Force
  - Attempts to guess a password by trying all possible character combinations
  - To defend, you should require strong passwords, limit failed login attempts, and audit login attempts

Common Types of Attacks (cont'd)

- Buffer Overflows
  - Forces strings that are longer than the max buffer size to be written to the buffer
  - Overflow can cause a program crash that leaves an unauthorized security level
  - A popular attack because there are so many programs with this vulnerability
- Denial of Service
  - Disrupts the ability of authorized users to access data
  - Usually either involves flooding a target with too many requests or sending a particular type of packet

Common Types of Attacks (cont'd)

- Man-in-the-Middle
  - An attacker listens between a user and a resource and intercepts data
- Social Engineering
  - An attacker convinces an authorized user to disclose information or allow unauthorized access
- System Bugs
  - Not an attack but offers vulnerabilities that can be exploited
  - Be careful with program development and apply patches for externally developed software

Unauthorized Access to Sensitive Information

- Final goal of many attacks is to gain access to sensitive information
- The attacker may wish to view, disclose, or modify information
- To avoid serious damage, protect data
  - Use appropriate controls
  - Be prepared to handle attacks that do occur

Summary

- An attack is an attempt to gain unauthorized access or to deny authorized access to a system
- An attacker is any individual or group who attempts to overcome a system's security controls
- A computer crime occurs when an attacker violates a law or regulation
- There are several broad categories of attacks
  - Military and intelligence, business, financial, terrorist, grudge, and fun

Summary (cont'd)

- A security incident is any violation of a security policy
- To deal with security incidents, you must
  - Understand the security policy and what activity would constitute an incident
  - Recognize the occurrence of an incident
  - Follow procedures to document and analyze the incident
  - Possibly follow through with legal action if necessary
- There are several categories of incidents
  - Scanning, compromise, malicious code, denial of service

Summary (cont'd)

- A good practice is to have a standing incident response team
- There are several types of malicious code
  - Viruses, worms, logic bombs, Trojan horses, issues of active content
- Common types of attacks include
  - Back doors, brute force, buffer overflows, denial of service, man-in-the-middle, social engineering, system bug exploitation

Assignments

- Reading: Chapter 7
- Practice 7.13 Challenge Questions
- Turn in Challenge Exercise 7.3 next week