SE 4C03 Winter 2006

06 Information Security

Instructor: W. M. Farmer

Revised: 8 February 2006

The Information Age

- Information drives commerce and culture
- Made possible by modern computing and communication technology
- Key infrastructure: **Internet**

A New Landscape

- World Wide Web
  - The Web is becoming a universal library
  - Nearly all **new** public information will be on the Web
- Commerce
  - Information is a major commodity
  - Information systems are a major tool of commerce
- Property
  - Much property is now digital
  - Who owns this digital property?
  - Who owns the metadata about digital property?
- Privacy
  - Privacy is threatened by the new technology
  - Encryption may enable some privacy to be preserved

A New Landscape (cont.)

- Risks
  - Much of the economy depends on computer networks and software
  - Many systems of our economy are tied together
- Crime
  - Crime can be perpetrated electronically from a distance
  - National borders are no longer a major obstacle to crime
- Warfare
  - Future wars may involve attacks on information systems instead of on military resources
  - Small countries and groups can attack large countries

Information Security

- Concerned with the protection of:
  - Electronically stored and manipulated information
  - The systems used to store and manipulate information
- Growing, dynamic field
  - Has major importance in the information age
  - **Network security** is an important subfield
- Closely related to the problem of software reliability
  - Information systems and security mechanisms are heavily based on software
  - Software is difficult to develop and maintain and very often unreliable

Why is Information Security Unique?

- Concerned with **misuse** instead of **proper use**

- Hard to engineer
  - Involves most components of an information system
  - Information security requirements clash with many other system requirements
  - Cuts across component boundaries and levels of abstraction

- A system is only as secure as its weakest component

What Needs to be Protected?

- Data
  - Privacy
  - Integrity
  - Availability
- Information systems
  - System privacy
  - System integrity
  - Availability of services
  - System resources (disk storage, CPU cycles, etc.)
  - Auditing
- Your personal and organization's reputation

Where do the Threats Come From?

- Software and configuration mistakes
- Hardware failures
- Operational mistakes
- Mobile code and viruses
- Insiders
- Hackers
- Information terrorists
- Natural disasters

What is a Security Policy?

- States what services and behavior are allowed and disallowed
- Prioritizes what is allowed and disallowed
- Specifies how violations will be dealt with
- Should be a written document available to all members of the organization

What is a Security Posture?

- The protective measures that are in place

- Should enforce the chosen security policy

- Includes both:
  - **Security strategies** (e.g., host protection, firewall, access control based on trust, monitor and react)
  - **Security mechanisms** (e.g., password protection, encryption, firewall devices)

Steps for Developing a Security Policy

1. Determine what are the operational and legal requirements of the information system

2. Decide what resources need to be protected

3. Determine what are the threats to these resources

4. Decide what entities will be trusted and to what degree

Note: The information used to develop a security policy should usually not be part of the security policy

Steps for Developing a Security Posture

1. Formulate a security policy

2. Determine what security resources are available

    - Financial resources
    - Hardware and software
    - Personnel
    - Outside expertise

3. Design and implement a security posture that satisfies the security policy using the resources above

General Principles

1. Have a **security policy** for the site or organization.

2. Keep the security policy and posture **simple**.

3. Prevent the information and security systems from being **probed**.

4. Give each subject the **least privilege** that is needed for it to perform its task.

5. Employ a **layered and diversified defense**.

General Principles (cont.)

6. Employ **choke points** to narrow the means and place of attack.

7. Make the information and security systems as **failsafe** as possible.

8. Require that all the information systems and all the personnel using them **participate** in the security strategy.

9. **Monitor** the information and security systems.

10. **Secure the security systems**.

Multilevel Security

- Each subject and object is assigned a security level

- The security levels form a lattice

- **Bell-LaPadula security model**:
  - A subject may not read objects higher than its assigned security level
  - A subject may not write objects lower than its assigned security level

- Information transmitted via **covert channels** is a concern

- The U.S. Department of Defense has spent many millions on this idea

Kinds of Threats

- Physical threats to hardware
- Faulty software
- Malicious software
- Unauthorized access
- Denial of service attacks
- Network probing
- Network manipulation
- Resource theft

Physical Threats to Hardware

- Hardware theft

- Hardware damage

- Unauthorized physical access to hardware

Faulty Software

- Malfunctioning software
  - Poorly designed (does not meet requirements)
  - Poorly implemented (does not meet specification)
- Software with exploitable bugs
  - Operating system releases
  - Software allowing buffer overflow
- Software with exploitable weaknesses
  - Flawed communication protocols
  - Network services
- Misconfigured software
  - Operating system security mechanisms
  - Web servers

Malicious Software

- A **virus** makes copies of itself and may be malicious in various ways

- A **worm** spreads across networks and may be malicious in various ways

- A **Trojan horse** has a hidden, illicit function

- A **logic bomb** has a hidden behavior that goes off when certain conditions are satisfied

- A **hacker's toolkit** is a collection of programs that enable one to probe and attack computers and networks

Unauthorized Access

- Surmount authentication
  - Password guessing
  - Password interception
  - Password cracking
  - Session replaying
- Session hijacking
- Identity spoofing
  - Source address spoofing
  - Domain name spoofing
- Misconfigured access control
  - SUID (Set User ID on execution) programs and scripts
  - SGID (Set Group ID on execution) programs and scripts

Denial of Service Attacks

- Overload a host or network
  - SYN flood: send to a host a flood of packets that request the creation of TCP connections
  - Broadcast storm
  - E-mail attacks
  - Virus and worm attacks
  - Process overload attacks

- Disable a host or network
  - Disk partition attacks (/, `/var`, `/tmp`, swap)
  - ICMP-based attacks

Network Probing

- Network probing tools
  - Ping
  - Traceroute

- Port scanning
  - TCP SYN scanning
  - TCP SYN half scanning
  - TCP FIN scanning

- Network analysis tools such as SATAN

- DNS

Network Manipulation

- Routing modification
  - Routing protocols without authentication such as the Routing Information Protocol (RIP)
  - ARP
- DNS modification
- Source routing
- Packet sniffing

Resource Theft

- CPU cycles
- Disk space
- Hosts
- Communication resources
- Self-beneficial attacks that unfairly increase the throughput of data
    - Example: TCP Daytona, S. Savage, 1999