CS 3CN3 and SE 4C03 Winter 2008

06 Information Security

William M. Farmer

Department of Computing and Software
McMaster University

12 February 2008

The Information Age

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

The New Information World (1)

- World Wide Web.
  - The Web has become a universal library.
  - Example: The Wikipedia has eclipsed the Encyclopaedia Britannica as the most important encyclopedic source of information.
  - Essentially all new public information is put on the Web.
  - There are several projects to put vast amounts of old information on the Web.
  - Example: Google's agreements with five major libraries (Harvard, University of Michigan, New York Public Library, Oxford, and Stanford).
- Commerce.
  - Information is now a major commodity.
  - Information systems are a major tool of commerce.

The New Information World (2)

- Digital Property.
  - Much property is now digital.
  - Examples include books, articles, news, music, video, and software.
  - Digital property can be reproduced almost instantaneously at extremely low cost.
- Information Ownership
  - Who should own intellectual and digital property?
  - Example: Myriad Genetics is fighting to keep hold of a patent for two breast cancer genes.
  - Who should own the metadata about intellectual and digital property?
- Privacy.
  - Privacy is threatened by the new technology.
  - Example: Identity theft.
  - Encryption may enable some privacy to be preserved.

The New Information World (3)

- Risks.
  - Much of the economy depends on computer networks and software.
  - Many systems of our economy are tied together.
- Cybercrime.
  - Crime via the computer and communication networks is a new development of major concern.
  - Example: Original design of the Internet infrastructure is inadequate.
  - Crime can be perpetrated electronically from a distance.
  - National borders are no longer a major obstacle to crime.
- Information Warfare.
  - Warfare may now include attacks on information systems (possibly instead of on military resources).
  - Example: May 2007 cyberattack on Estonia.
  - 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.
  - Hard to separate from other concerns.
- A system is only as secure as its weakest component.

What Needs to be Protected?

1. Data.
   - Confidentiality.
   - Integrity.
   - Availability.
2. Information systems.
   - System confidentiality.
   - System integrity.
   - Availability of services.
   - System resources (disk storage, CPU cycles, etc.).
   - Monitoring mechanisms.
   - Security mechanisms.
3. Your personal and organization's reputation.

Confidentiality

- Confidentiality (also called privacy) is the state in which information or resources are concealed.
- Confidentiality also applies to metadata about information and resources.
  - Examples include existence, location, protection, etc.
- Confidentiality is achieved by following the need to know principle, a special case of the principle of least privilege.
- Military interest in keeping information secret was the main driving force behind the development of mechanisms to achieve confidentiality in the years between World War II and the advent of the Internet.

Integrity

- Integrity is the state in which data or resources have not been accidently or maliciously modified or destroyed.
- Integrity also applies to metadata about information and resources.
  - Examples include origin, provenance, access history, etc.
- An integrity violation reduces the trustworthiness of the data or resources.
- There are two approaches to maintain integrity:
  - Prevention of unauthorized attempts to modify the data or resources.
  - Detection of integrity violations or unauthorized modifications.
- The banking industry has been a major player in the development of mechanisms to achieve integrity.

Availability

- Availability is the state in which information or resources can be used as needed.
- Availability is an important aspect of reliability.
- Denial of service attacks are attempts to block availability.
  - They are difficult to detect because they can look like legitimate, but possibly atypical, attempts to access information and resources.

Threats and Attacks

- A threat is a potential violation of confidentiality, integrity, or availability.
- An attack is an attempt to violate confidentiality, integrity, or availability.

Kinds of Threats

- System failure.
- System modification.
- Resource theft.
- Vandalism.
- System probing.
- Unauthorized access.
- Repudiation of origin.
- Denial of receipt.
- Delay.
- Denial of service.

Where do the Threats Come From?

- Faulty hardware.
- Faulty software.
- Configuration mistakes.
- Operational mistakes.
- Insiders.
- Hackers.
- Criminals, vandals, and terrorists.
- Malicious code (such as viruses).
- Natural disasters.

Physical Threats to Hardware

- Hardware theft.
- Hardware damage.
- Unauthorized physical access to hardware.

Threats from 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 Trojan horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect.
- A computer virus is a program that inserts itself in one or more files and then performs some (possibly null) action.
- A computer worm is a program that copies itself from one computer to another.
- A computer bacterium is a program that absorbs all of some class of resource.
- A logic bomb is a program that performs a malicious action when some external event occurs.
- Mobile code is software that is intended to be moved from one computer to another.
- 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.
  - ICMP flood: send to a host a flood of ICMP packets (such as echo requests or echo replies).
  - 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 (such as the ping of death).

Network Probing

- Network probing tools.
  - Ping.
  - Traceroute.
- Port scanning (for open, closed, and filtered ports).
  - UDP scanning
  - TCP SYN scanning.
  - TCP SYN half scanning.
  - TCP FIN scanning.
  - TCP ACK 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.

Security Policies

- A security policy is a document that states what services and behavior are allowed and disallowed.
- The security policy for an organization defines what is meant by “security” within the organization.
- A security policy should be a written document available to all members of the organization.
- The composition of security policies is a concern: security vulnerabilities can occur if the security policies conflict.

Security Mechanisms

- A security mechanism is a method, tool, or procedure for enforcing a security policy (Bishop).
- An organization's security posture is the collection of security mechanisms that the organization has in place.
- A security system is a collection of coherent security mechanisms intended to enforce a security policy.

Security Strategies

- A security strategy is an approach to enforcing a security policy.
- Goals of a security strategy:

  1. Prevention: Prevent an attack from occurring.
  2. Detection: Detect an attack.
  3. Recovery: Stop an attack and then recover, or function as best as possible under an attack.

Assumptions

- Underlying every security policy are certain assumptions.
- Two principal assumptions are:

  1. The policy correctly and unambiguously partitions the set of system states into secure and nonsecure states.
  2. There exists a set of security mechanisms that will enforce the security policy.

Security Mechanisms

- Let s be a system such that P is the set of its possible states and $Q \subseteq P$ is the set of its secure states.
- Let m be a security mechanism and $R_m \subseteq P$ be the set of states to which s is restricted by m.
- m is secure if $R_m \subseteq Q$.
- m is precise if $R_m = Q$.
- m is broad if R_m is not secure.
- The goal of a security system is to behave as a single precise security mechanism.
- In practice security mechanisms are usually broad, allowing the system to enter some nonsecure states.

Trust and Assurance

- Trust is a measure of the confidence that a system satisfies its requirements.
- Assurance is evidence that a system satisfies its requirements.
- The more assurance a system has the more it is trusted.
- Assurance is established in three major steps:
  1. A specification of the requirements of the system is produced.
  2. A design is produced that satisfies the requirements specification of the system.
  3. An implementation is produced that satisfies the design of the system.

Operational Issues

- The selection of a security policy or security system requires a cost-benefit analysis.
  - The costs include the cost of developing security measures as well as the cost of security breaches.
- A risk analysis is needed to assess the likelihood of specific threats and the level of damage they would cause.
  - Risk is a function of environment and time.
  - Some risks may be considered acceptable.
- Security measures are constrained by both law and custom.

Human Issues

- Human issues play a major role in information security.
- Threats that have never happened are often hard for people to take seriously.
- Those who are responsible for security must be given the power needed to implement adequate security measures.
- Security needs adequate human and material resources.
- Personnel need adequate training and must understand the importance of security measures.
- Insiders should be carefully monitored.
- Measures should be taken to counter social engineering attacks.
- Human error should be expected.

Security Life Cycle

1. Threats
2. Policy
3. Security system development
    3.1 Requirements specification
    3.2 Design
    3.3 Implementation
    3.4 Operation and maintenance

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.
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.