Computer and Network Security

- Reference
  - "*Computer Security: Principles and Practice,*" 3/E, by William Stallings and Lawrie Brown, Prentice Hall
  - The PPT slides are created mainly based on the PPT slides provided by the authors of the textbook.
- Introduction
  - What is Computer Security
  - Types of attacks
  - Countermeasures

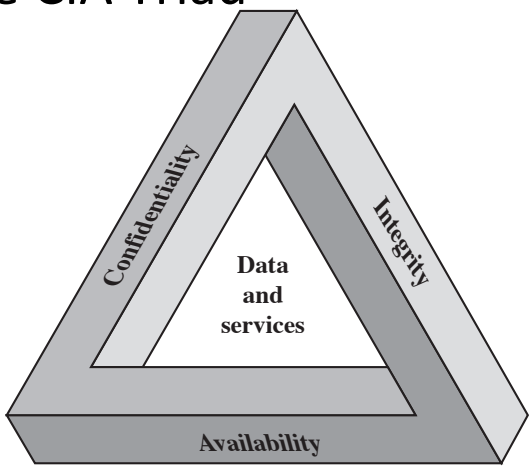
What is Computer Security

The ***NIST Computer Security Handbook*** defines the term Computer Security as:

"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability** and **confidentiality** of information system resources" (includes hardware, software, firmware, information/data, and telecommunications).

The CIA Triad

- Confidentiality
  - data confidentiality
  - privacy
- Integrity
  - data integrity
  - system integrity
- Availability



For example, the NIST standard FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems) lists confidentiality, integrity, and availability as the three* security objectives for information and for information systems.

Characterization: Requirements (FIPS PUB 199)

Confidentiality

- **preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information**

Integrity

- **guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity**

Availability

- **ensuring timely and reliable access to and use of information**

Two More Key Objectives

- **Authenticity:**
  - The property of being genuine and being able to be verified and trusted;
  - confidence in the validity of a transmission, a message, or message originator.
- **Accountability:**
  - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Computer Security Challenges

- Computer security is not as simple as it might first appear to the novice
- Potential attacks on the security features must be considered
- Procedures used to provide particular services are often counterintuitive
- Physical and logical placement needs to be determined
- Additional algorithms or protocols may be involved
- Attackers only need to find a single weakness, the developer needs to find all weaknesses
- Users and system managers tend to not see the benefits of security until a failure occurs
- Security requires regular and constant monitoring
- Is often an afterthought to be incorporated into a system after the design is complete
- Thought of as an impediment to efficient and user-friendly operation

Adversary (threat agent)
An entity that attacks, or is a threat to, a system.

Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)
Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Table 1.1
Computer Security Terminology

- RFC 4949, Internet Security Glossary, May 2000

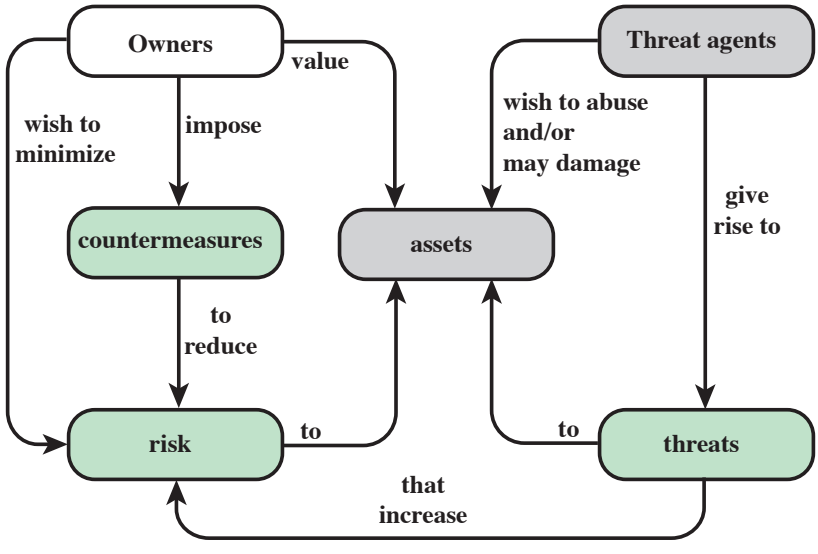
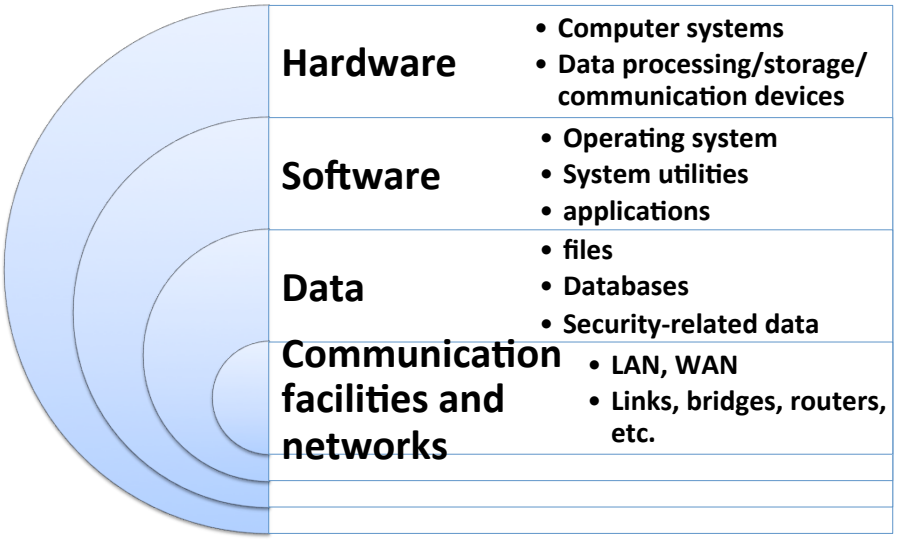


Figure 1.1 Security Concepts and Relationships

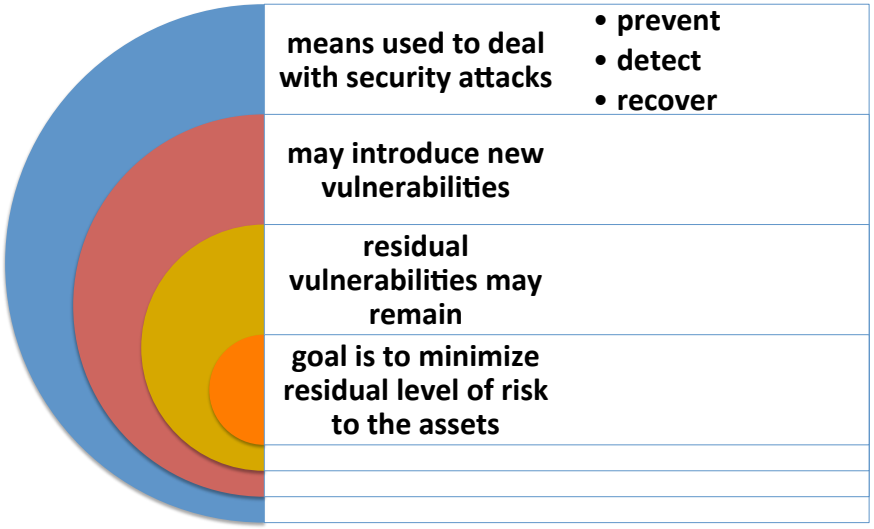
Assets of a Computer System



Vulnerabilities, Threats, and Attacks

- categories of vulnerabilities
  - corrupted (loss of integrity)
  - leaky (loss of confidentiality)
  - unavailable or very slow (loss of availability)
- threats
  - capable of exploiting vulnerabilities
  - represent potential security harm to an asset
- attacks (threats carried out)
  - passive – does not affect system resources
  - active – attempt to alter system resources or affect their operation
  - inside – initiated by an entity inside the security parameter
  - outside – initiated from outside the perimeter

Countermeasures



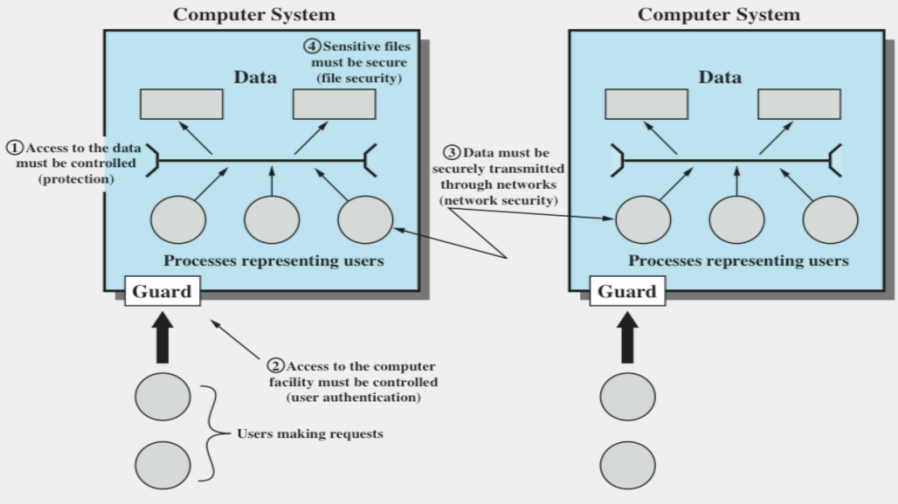


Figure 1.2 Scope of Computer Security. This figure depicts security concerns other than physical security, including control of access to computers systems, safeguarding of data transmitted over communications systems, and safeguarding of stored data.

Assets and Examples of Threats

	Availability	Confidentiality	Integrity
Hardware			
Software			
Data			
Communication Lines and Networks			

Messages are read. The traffic pattern of messages is observed.

An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.

A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.

Existing files are modified or new files are fabricated.

Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

An unencrypted CD-ROM or DVD is stolen.

Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.

Equipment is stolen or disabled, thus denying service.

Programs are deleted, denying access to users.

An unauthorized copy of software is made.

Files are deleted, denying access to users.

Assets and Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Passive and Active Attacks

- Passive attacks attempt to learn or make use of information from the system but does not affect system resources
  - eavesdropping/monitoring transmissions. Two types:
    - release of message contents
    - traffic analysis
  - difficult to detect
  - emphasis is on prevention rather than detection
- Active attacks involve modification of the data stream
  - four categories:
    - replay
    - masquerade
    - modification of messages
    - denial of service
  - goal is to detect them and then recover

FIPS PUB 200 Security Requirements

Access control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and training: (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and accountability: (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, accreditation, and security assessments: (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration management: (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency planning: Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and authentication: Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident response: (i) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance: (i) Perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media protection: (i) Protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and environmental protection: (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel security: (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk assessment: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Systems and services acquisition: (i) Allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and communications protection: (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and information integrity: (i) Identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Security Functional Requirements

Areas requiring computer security technical measures	Areas requiring management controls & procedures	Areas requiring both
• access control • identification & authentication • system & communication protection • system & information integrity	• awareness & training • audit & accountability • certification, accreditation, & security assessments • contingency planning • maintenance • physical & environmental protection • planning • personnel security • risk assessment • systems & services acquisition	• configuration management • incident response • media protection

Computer Security Strategy

- Security Policy
  - Formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
- Security Implementation
  - Involves four courses of action: prevention, detection, response, recovery
- Assurance
  - The degree of confidence one has that the security measures work as intended
- Evaluation
  - Process of examing a computer product or system with respect to certain criteria.