Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 1

Overview

The NIST Internal/Interagency Report NISTIR 7298 (*Glossary of Key Information Security Terms* , May 2013) defines the term *computer security* as follows:

" Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of information system assets including hardware, software, firmware, and information being processed, stored, and communicated."

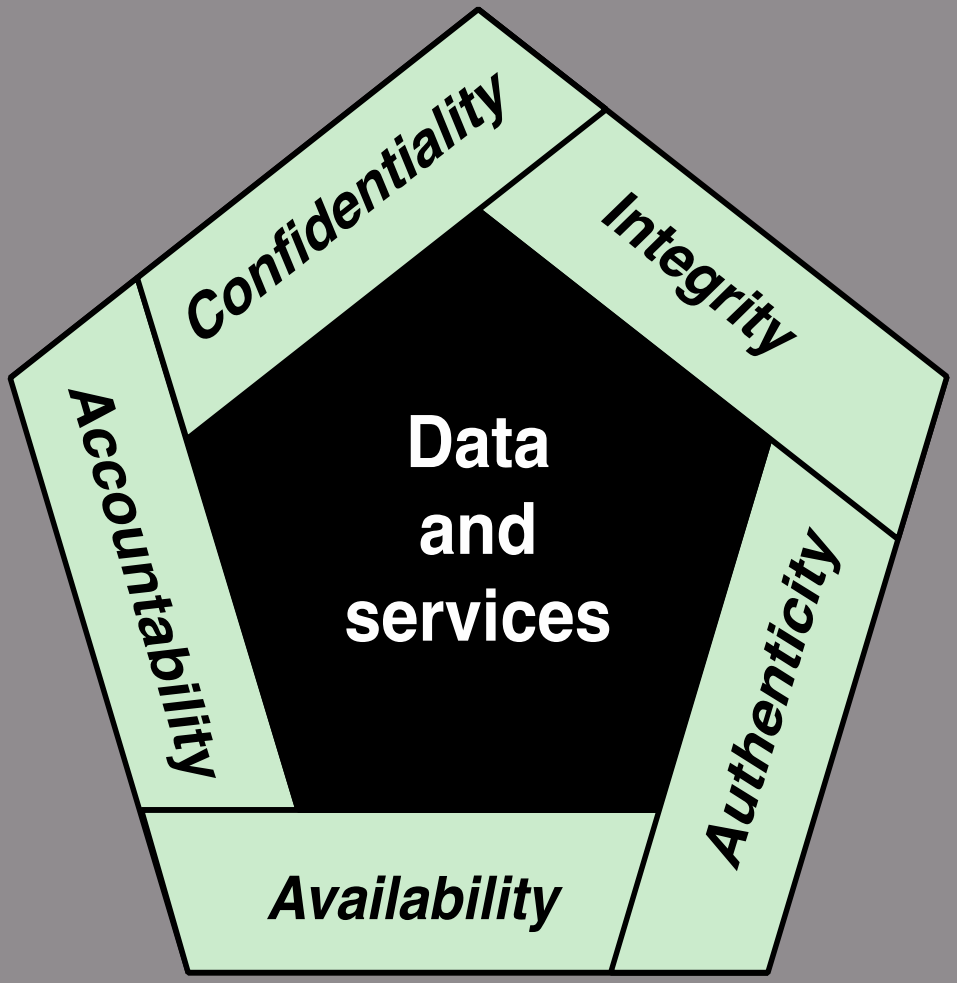


Figure 1.1 Essential Network and Computer Security Requirements

Key Security Concepts

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

Levels of Impact

Low

The loss could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals

Moderate

The loss could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals

High

The loss could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals

Computer Security Challenges

1. Computer security is **not as simple as it might first appear** to the novice
2. In developing a particular security mechanism or algorithm, one must always consider **potential attacks** on those security features
3. Procedures used to provide particular services are often **counterintuitive**
4. Physical and logical **placement** needs to be determined
5. Security mechanisms typically **involve more than a particular algorithm or protocol** and also require that participants be in possession of some **secret information** which raises questions about the creation, distribution, and protection of that secret information
6. **Attackers** only need to **find a single weakness**, while the **designer** must **find and eliminate all weaknesses** to achieve perfect security
7. Security is still too often an **afterthought** to be incorporated into a system after the design is complete, rather than being an integral part of the design process
8. Security requires regular and constant **monitoring**
9. There is a natural tendency on the part of users and system managers to perceive **little benefit** from security investment until a security failure occurs
10. Many users and even security administrators view strong security as an **impediment** to efficient and user-friendly operation of an information system or use of information

Table 1.1

Computer Security Terminology, from RFC 2828, *Internet Security Glossary*, May 2000

Adversary (threat agent)
Individual, group, organization, or government that **conducts or has the intent to conduct detrimental activities**.

Attack
Any kind of **malicious activity** that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Countermeasure
A device or techniques that has as its objective **the impairment of the operational effectiveness of undesirable or adversarial activity**, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Risk
A measure of **the extent to which an entity is threatened** by a potential circumstance or event, and typically a function of 1) **the adverse impacts** that would arise if the circumstance or event occurs; and 2) **the likelihood of occurrence**.

Security Policy
A set of criteria for the provision of security services. It **defines and constrains the activities** of a data processing facility in order to maintain a condition of security for systems and data.

System Resource (Asset)
A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be **exploited or triggered by a threat source**.

(Table can be found on page 8 in the textbook)

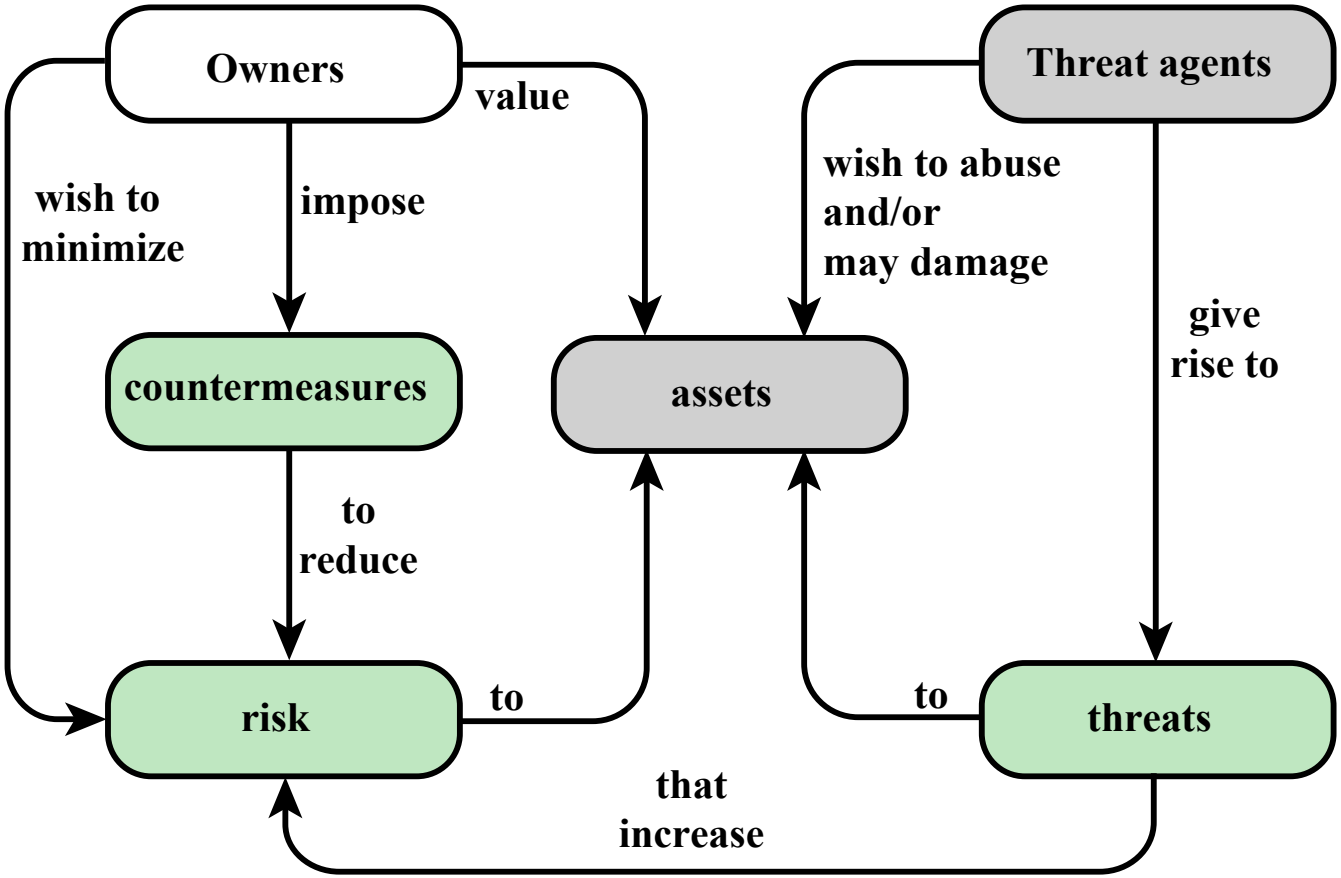
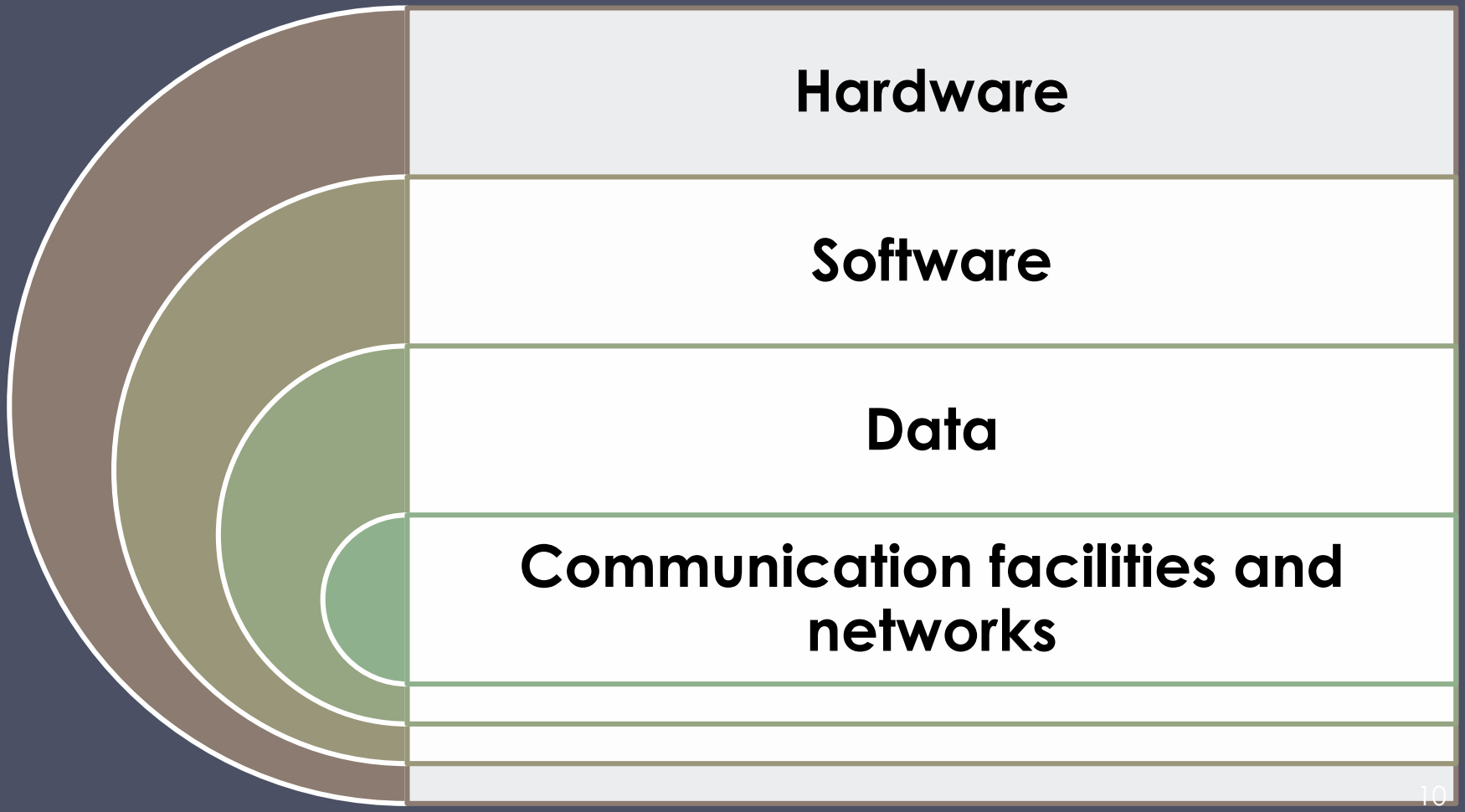


Figure 1.2 Security Concepts and Relationships

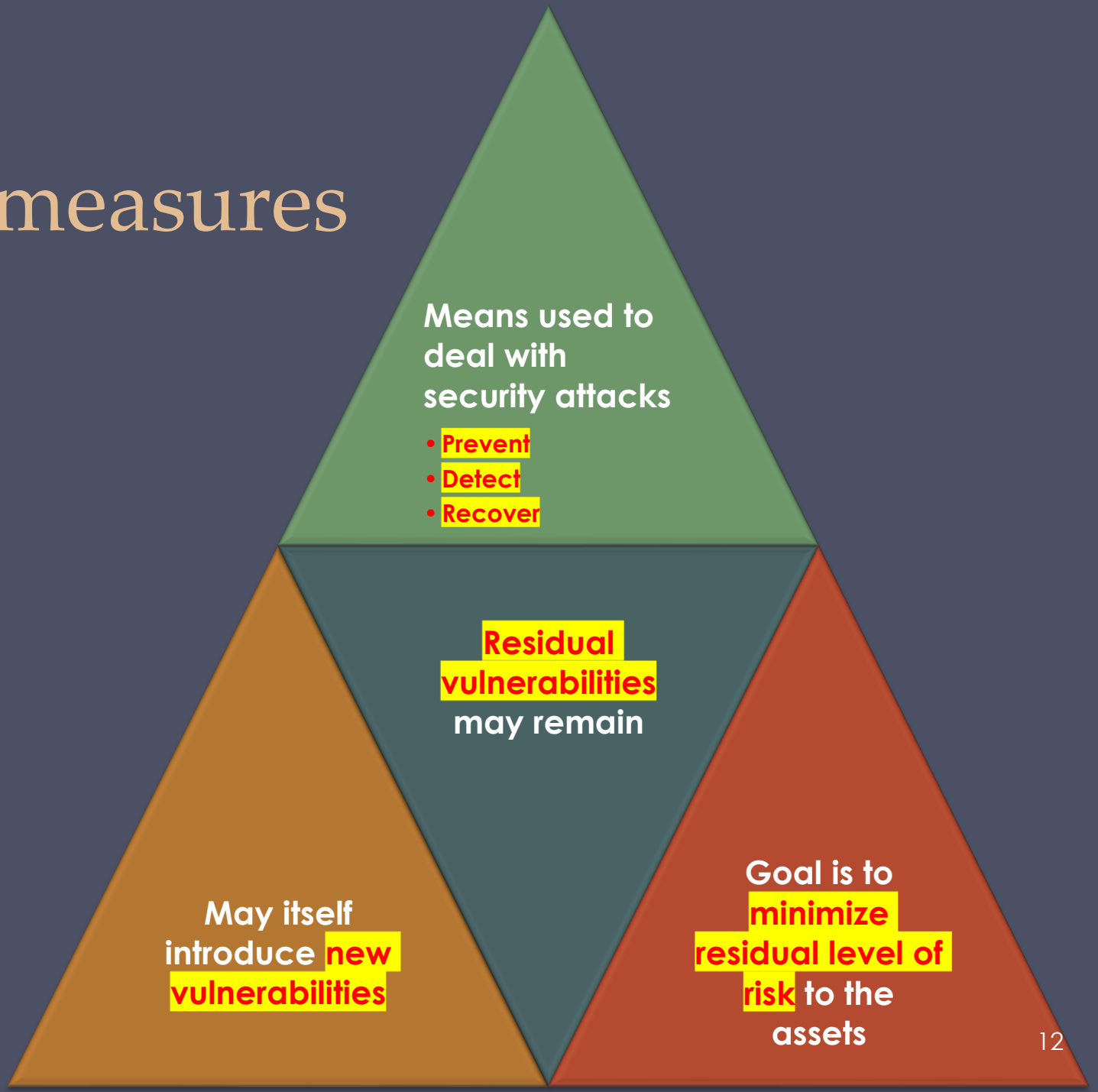
Assets of a Computer System



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** – attempt to learn or make use of information from the system that does not affect system resources
  - **Active** – attempt to alter system resources or affect their operation
  - **Insider** – initiated by an entity inside the security perimeter
  - **Outsider** – initiated from outside the perimeter

Countermeasures



Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security

Table 1.2

Threat Consequences, and the Types of Threat Actions That Cause Each Consequence

Based on RFC 4949

**Table is on page 10 in the textbook.

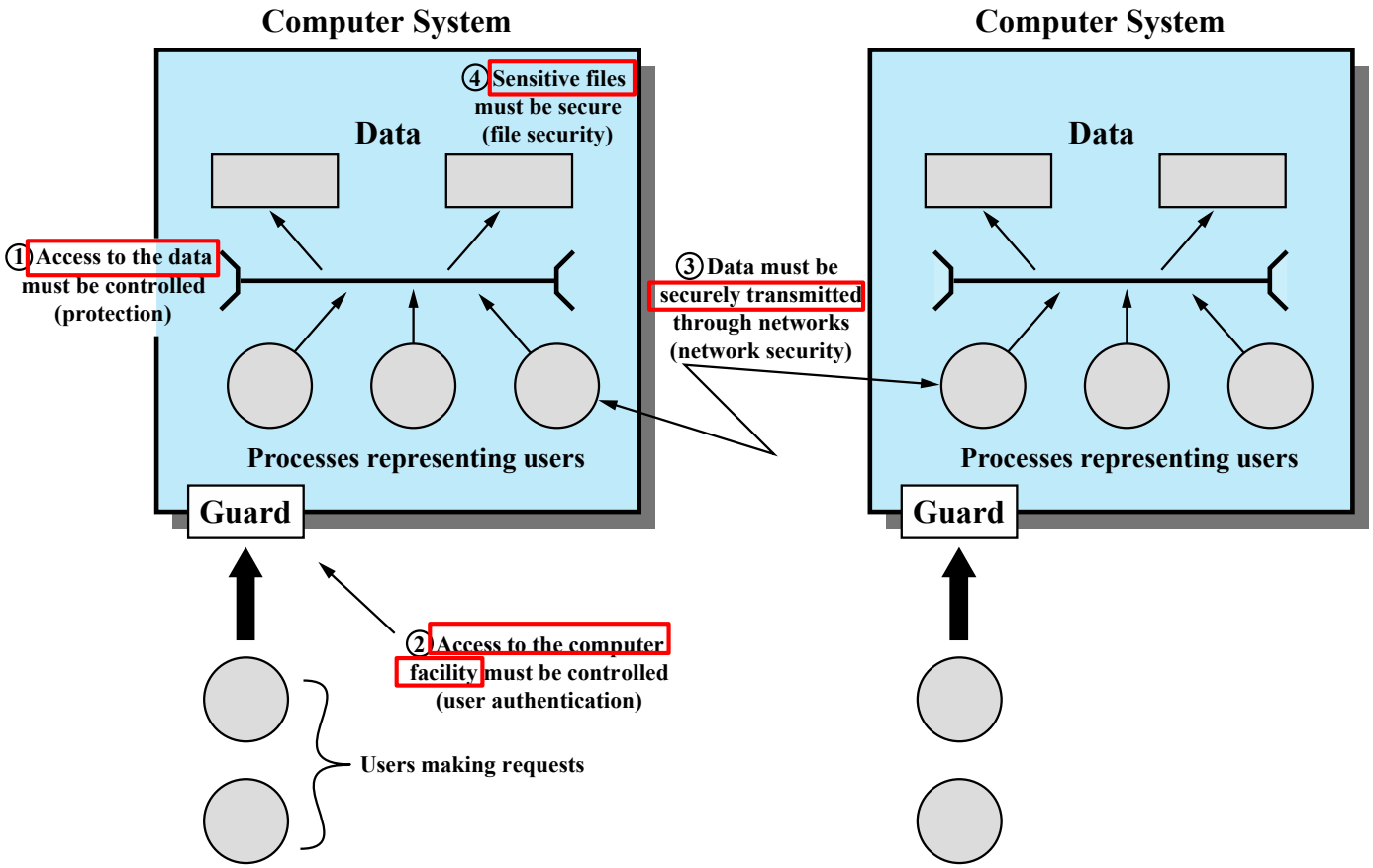


Figure 1.3 Scope of Computer Security. This figure depicts security concerns other than physical security, including control of access to computers systems, safeguarding of data transmitted over communications systems, and safeguarding of stored data.

Table 1.3
Computer and Network Assets, with 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 Attack

- Attempts to learn or make use of information from the system but **does not affect system resources**
- **Eavesdropping** on, or **monitoring** of, transmissions
- Goal of attacker is to **obtain information** that is being transmitted
- Two types:
  - Release of **message contents**
  - **Traffic analysis**

Active Attack

- Attempts to **alter** system resources or **affect** their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - **Replay**
  - **Masquerade**
  - **Modification** of messages
  - **Denial of service**

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.

Table 1.4

Security Requirements

(FIPS 200)

(page 1 of 2)

(Table can be found on pages 16-17 in the textbook.)

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.

Table 1.4

Security Requirements

(FIPS 200)

(page 2 of 2)

(Table can be found on pages 16-17 in the textbook.)

Fundamental Security Design Principles

Economy of mechanism	Fail-safe defaults	Complete **mediation**	Open design
Separation of privilege	**Least privilege**	**Least common** mechanism	**Psychological** acceptability
Isolation	**Encapsulation**	**Modularity**	**Layering**

Least astonishment

Attack Surfaces

Consist of the **reachable** and **exploitable** **vulnerabilities** in a system

Examples:

Open ports on outward facing Web and other servers, and **code** listening on those ports	**Services** available on the inside of a firewall	**Code** that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats	**Interfaces**, **SQL**, and **Web forms**	**An employee** with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories

Network Attack Surface

Vulnerabilities over an enterprise network, wide-area network, or the Internet

Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks

Software Attack Surface

Vulnerabilities in application, utility, or operating system code

Particular focus is Web server software

Human Attack Surface

Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

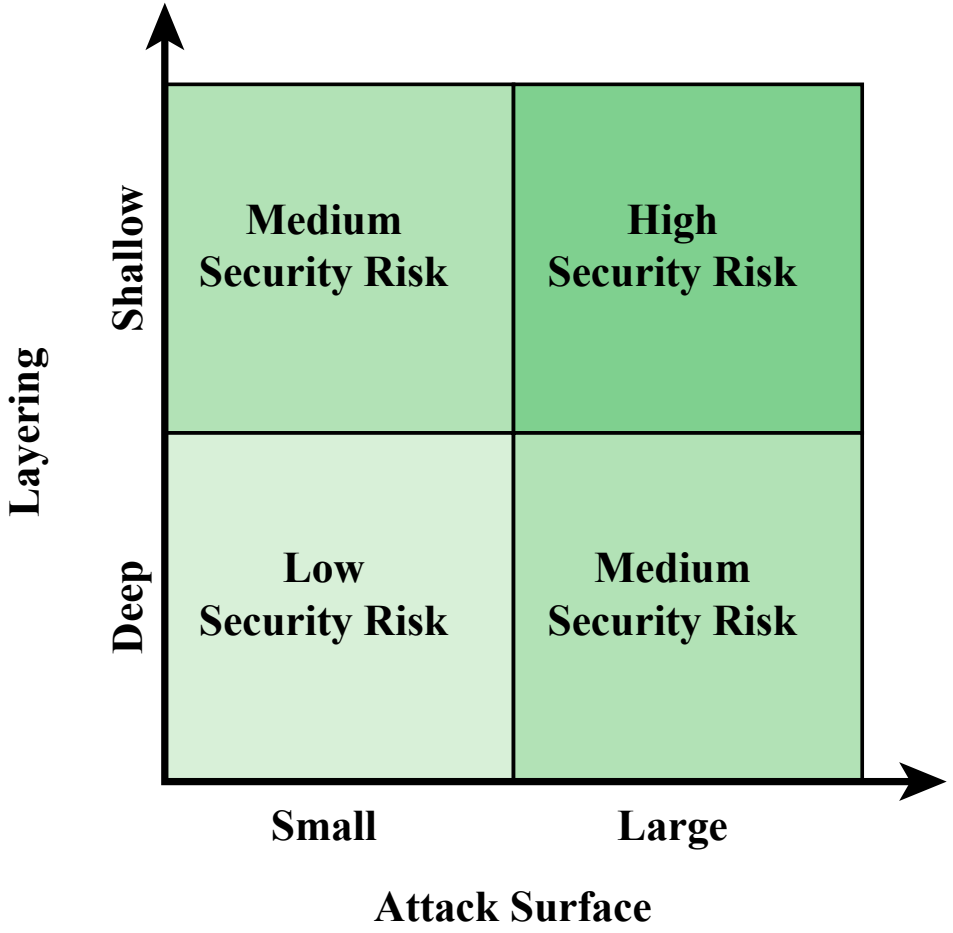


Figure 1.4 Defense in Depth and Attack Surface

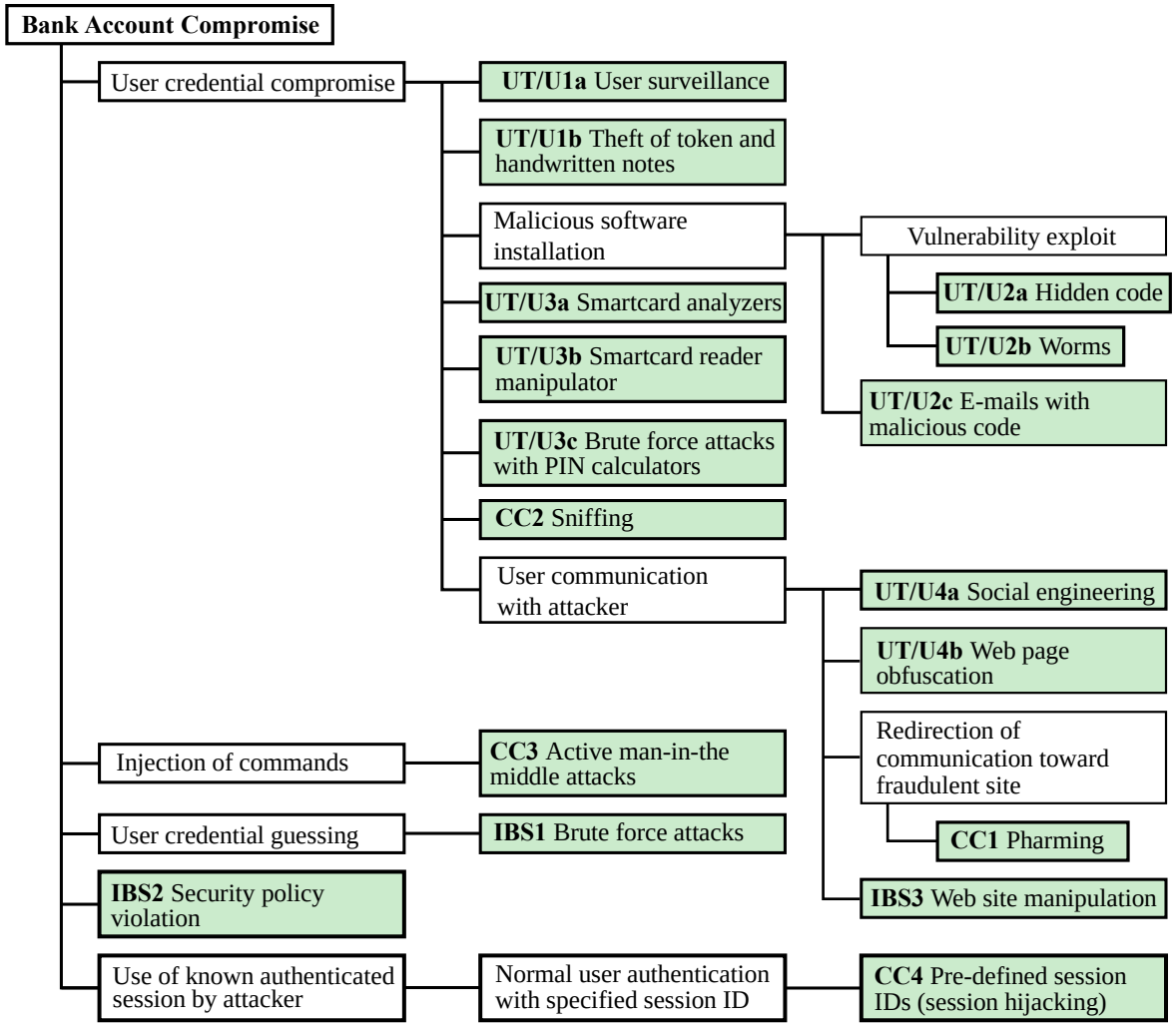


Figure 1.5 An Attack Tree for Internet Banking Authentication

Computer Security Strategy

Standards

- Standards have been developed to cover **management practices** and the overall architecture of **security mechanisms and services**
- The most important of these organizations are:
  - **National Institute of Standards and Technology (NIST)**
    - **NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation**
  - **Internet Society (ISOC)**
    - **ISOC is a professional membership society that provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards**
  - **International Telecommunication Union (ITU-T)**
    - **ITU is a United Nations agency in which governments and the private sector coordinate global telecom networks and services**
  - **International Organization for Standardization (ISO)**
    - **ISO is a nongovernmental organization whose work results in international agreements that are published as International Standards**

Summary

- Computer security concepts
  - Definition
  - Challenges
  - Model
- Threats, attacks, and assets
  - Threats and attacks
  - Threats and assets
- Security functional requirements
- Fundamental security design principles
- Attack surfaces and attack trees
  - Attack surfaces
  - Attack trees
- Computer security strategy
  - Security policy
  - Security implementation
  - Assurance and evaluation
- Standards

作业

- 教材（英文原版）P50-51 Problems 1.2，1.3，1.5，1.6