Information Security (CS3002)

Instructor: Dr. Muhammad Usama

Email: usama.khanzada@nu.edu.pk

Book: Computer Security - Principles and Practice (Chapter 1)

A definition of computer security

- **Computer security:** 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)

NIST 1995

Three key objectives (the CIA triad)

- **Confidentiality**
  - **Data confidentiality**: Assures that confidential information is not disclosed to unauthorized individuals
  - **Privacy**: Assures that individual control or influence what information may be collected and stored
- **Integrity**
  - **Data integrity**: assures that information and programs are changed only in a specified and authorized manner
  - **System integrity**: Assures that a system performs its operations in unimpaired manner
- **Availability**: assure that systems works promptly, and service is not denied to authorized users

Other concepts to a complete security picture

- **Authenticity**: the property of being genuine and being able to be verified and trusted; confident in the validity of a transmission, or a message, or its originator
- **Accountability**: generates the requirement for actions of an entity to be traced uniquely to that individual to support nonrepudiation, deference, fault isolation, etc.

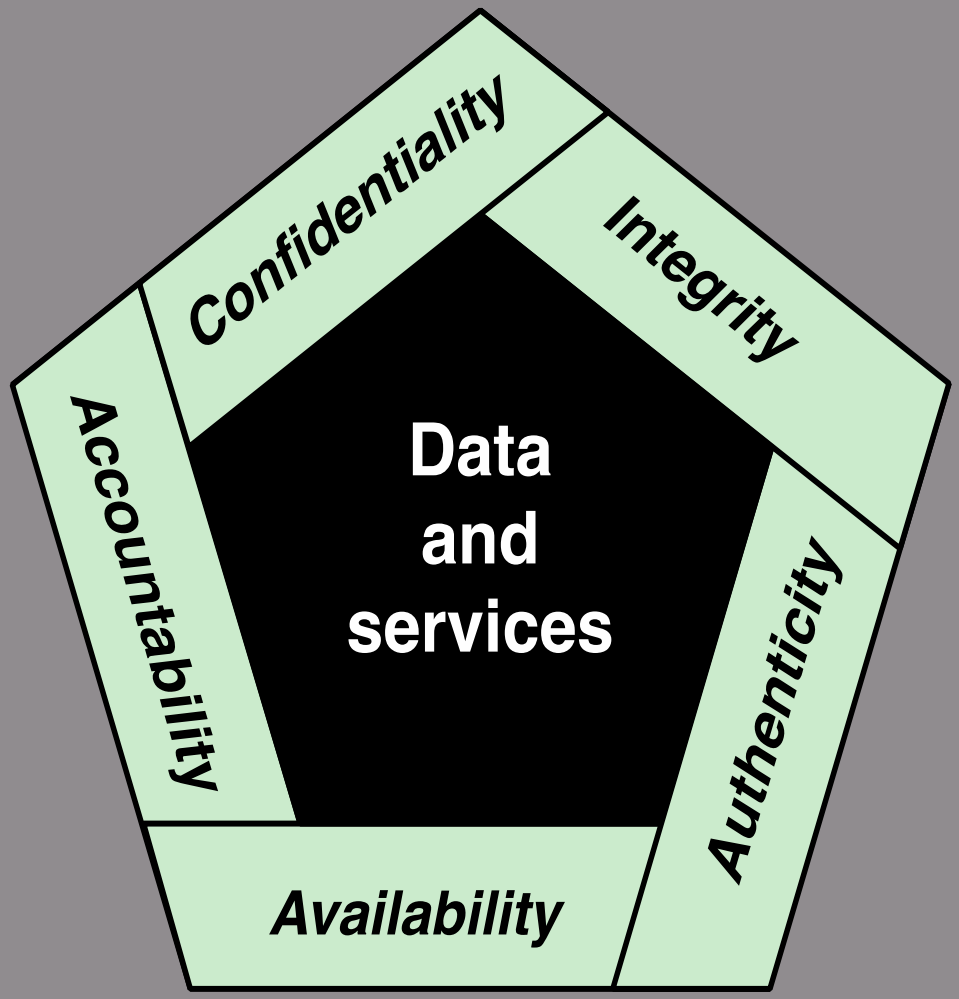


Figure 1.1 Essential Network and Computer Security Requirements

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

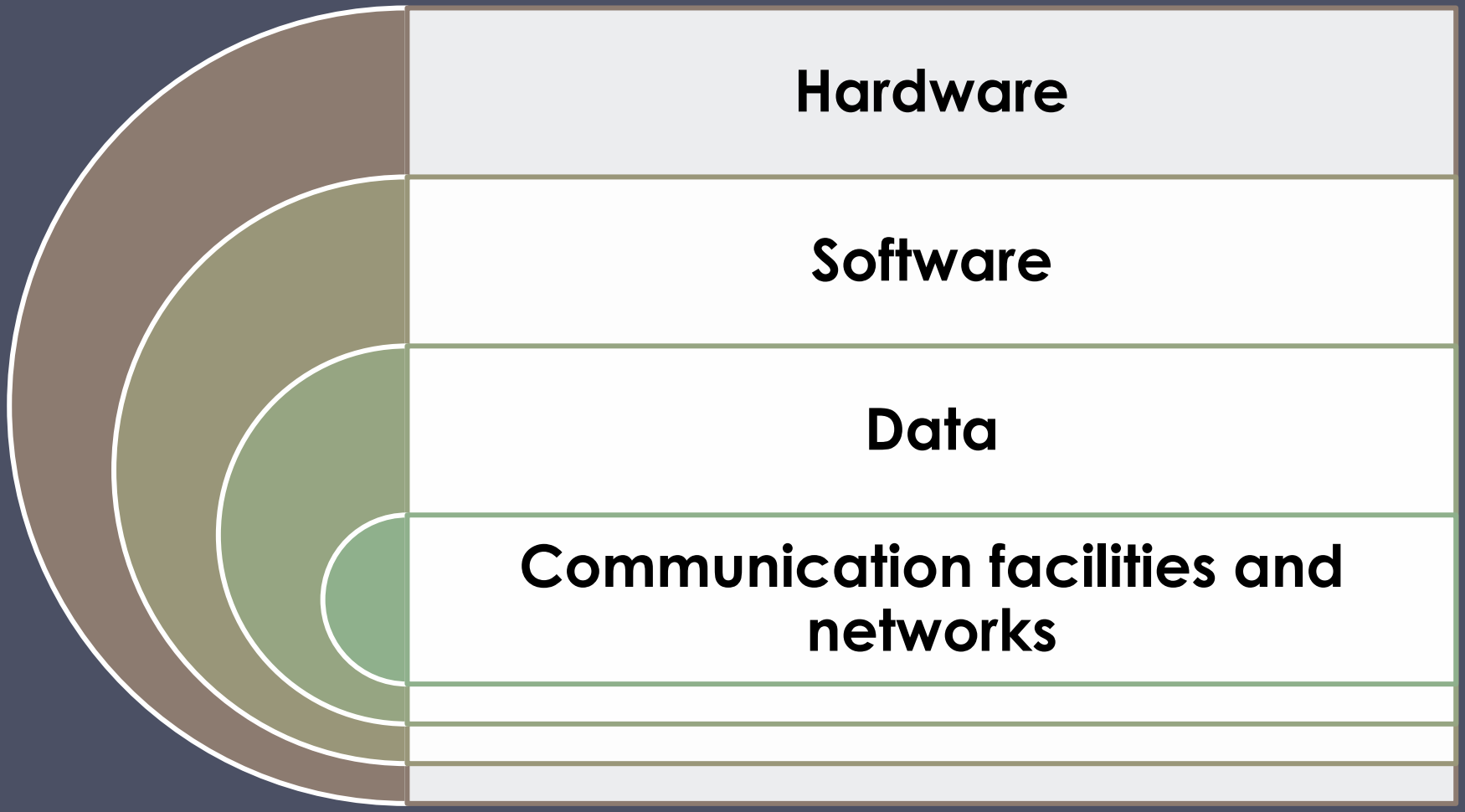
The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Challenges of computer security

1. Computer security is not simple
2. One must consider potential (unexpected) attacks
3. Procedures used are often counter-intuitive
4. Must decide where to deploy mechanisms
5. Involve algorithms and secret info (keys)
6. A battle of wits between attacker / admin
7. It is not perceived on benefit until fails
8. Requires constant monitoring
9. Too often an after-thought (not integral)
10. Regarded as impediment to using system

A model for computer security

Assets of a Computer System



Computer security terminology

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.

Computer security terminology (Cont..)

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.

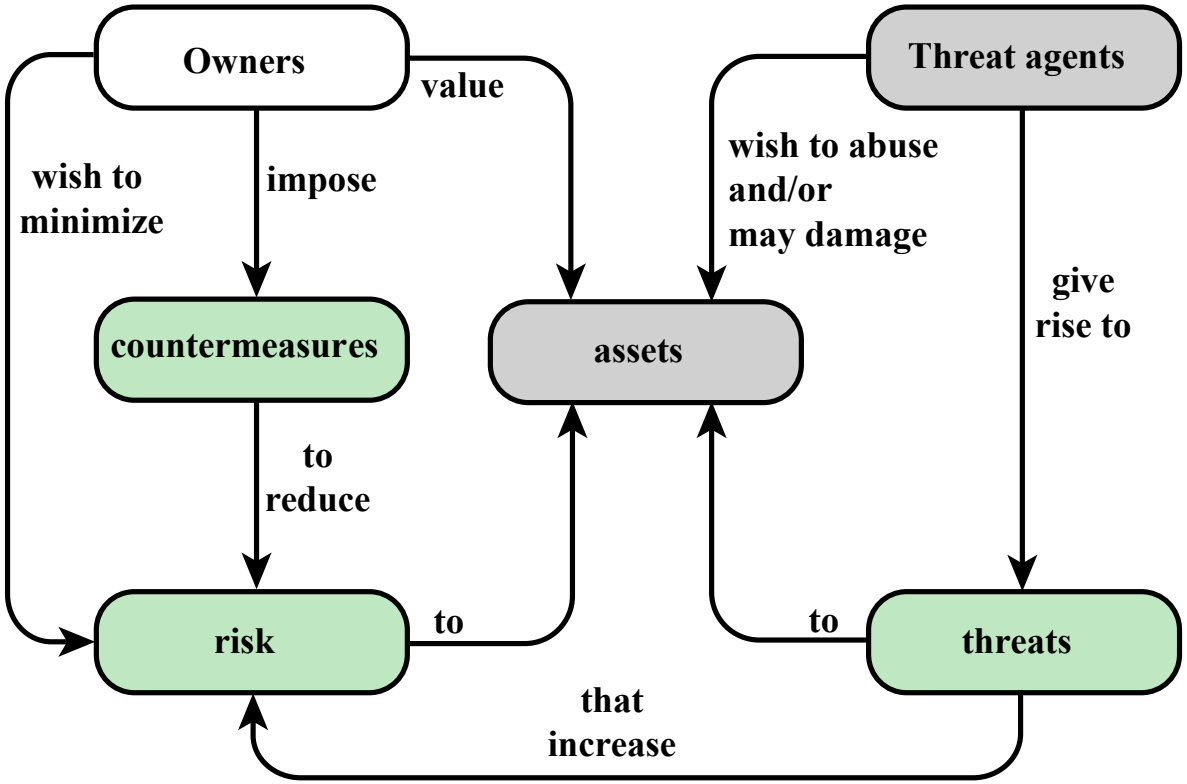
Threat

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.

Security concepts and relationships

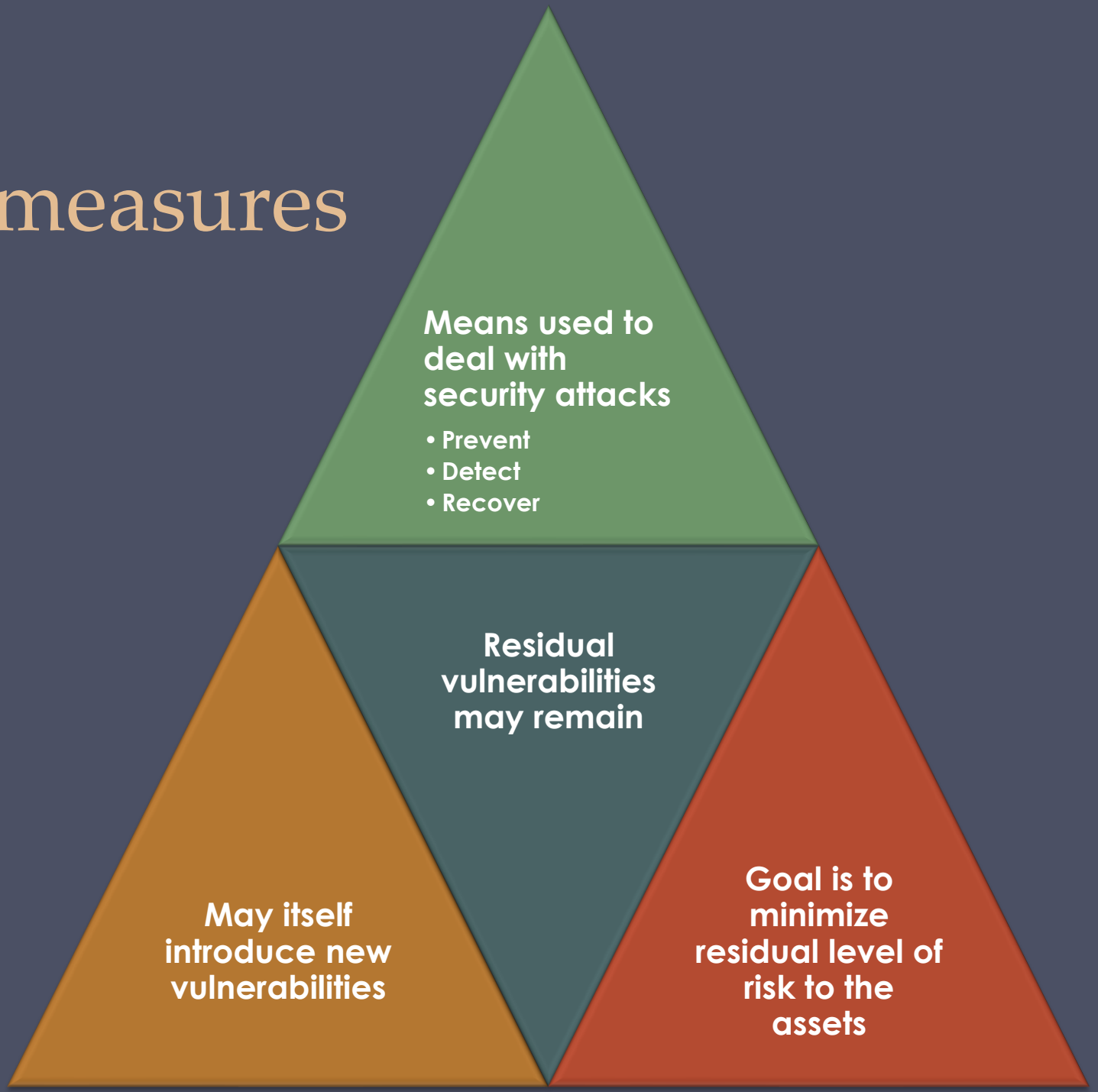


Threats, Attacks and Assets

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 parameter
  - Outsider – initiated from outside the perimeter

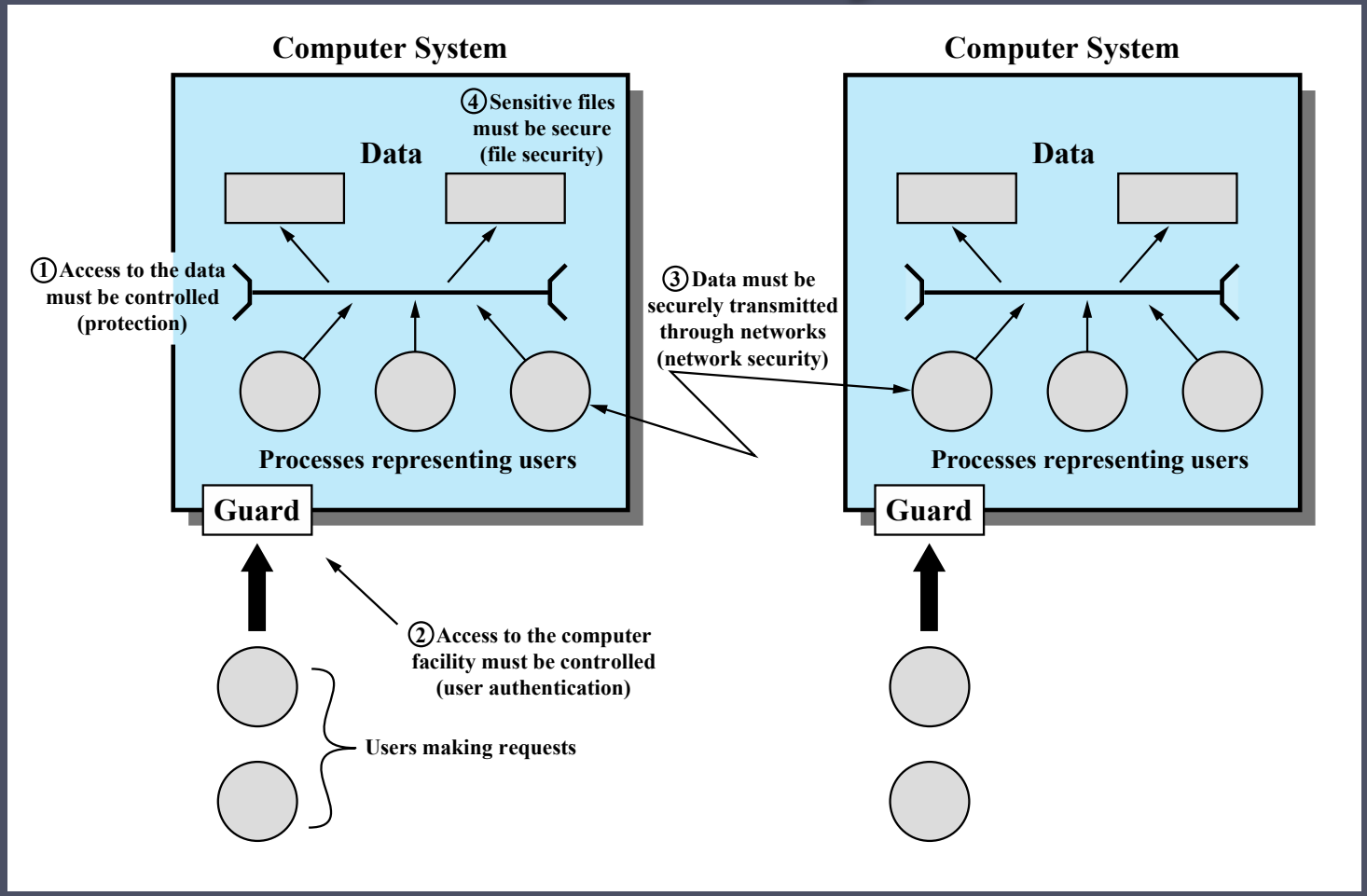
Countermeasures



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

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.

The scope of computer security



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.

Fundamental Security Design Principles

Fundamental Security Design Principles

- Despite years of research, it is still difficult to design systems that comprehensively prevent security flaws
- But good practices for good design have been documented (analogous to software engineering)

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	

Fundamental security design principles (Cont..)

- **Economy of mechanism**: the design of security measures should be as simple as possible
  - Simpler to implement and to verify
  - Fewer vulnerabilities
- **Fail-safe default**: access decisions should be based on permissions; i.e., the default is lack of access
- **Complete mediation**: every access should check against an access control system
- **Open design**: the design should be open rather than secret (e.g., encryption algorithms)

Fundamental security design principles (Cont..)

- **Isolation**
  - Public access should be isolated from critical resources (no connection between public and critical information)
  - Users files should be isolated from one another (except when desired)
  - Security mechanism should be isolated (i.e., preventing access to those mechanisms)
- **Encapsulation**: like object concepts (hide internal structures)
- **Modularity**: modular structure

Fundamental security design principles (Cont..)

- **Layering (defense in depth)**: use of multiple, overlapping protection approaches
- **Least astonishment**: a program or interface should always respond in a way that is least likely to astonish a user

Fundamental security design principles (Cont..)

- **Separation of privilege**: multiple privileges should be needed to do achieve access (or complete a task)
- **Least privilege:** every user (process) should have the least privilege to perform a task
- **Least common mechanism**: a design should minimize the function shared by different users (providing mutual security; reduce deadlock)
- **Psychological acceptability**: security mechanisms should not interfere unduly with the work of users

Computer security strategy

Computer security strategy

- An overall strategy for providing security
  - **Policy** (specs): what security schemes are supposed to do
    - Assets and their values
    - Potential threats
    - Ease of use vs security
    - Cost of security vs cost of failure/recovery
  - **Implementation/mechanism**: how to enforce
    - Prevention
    - Detection
    - Response
    - Recovery
  - **Correctness/assurance**: does it really work (validation/review)

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
- Standards
- Fundamental security design principles
- Computer security strategy
  - Security policy
  - Security implementation
  - Assurance and evaluation