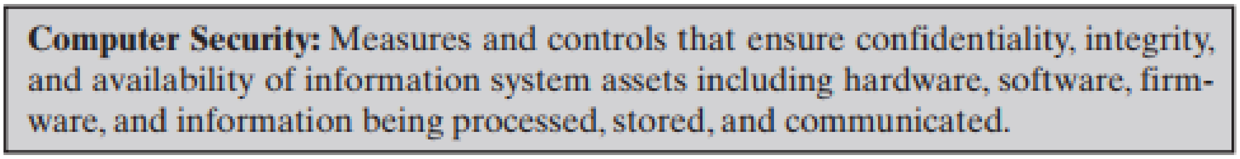
Chapter 1(1.1, 1.2, 1.4, 1.6, 1.7)



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

This definition introduces three key objectives that are at the heart of computer security:

Confidentiality: This term covers two related concepts:

- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- **Privacy**: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity: This term covers two related concepts:

- **Data integrity**: Assures that information and programs are changed only in a specified and authorized manner.
- **System integrity**: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability: Assures that systems work promptly and service is not denied to authorized users

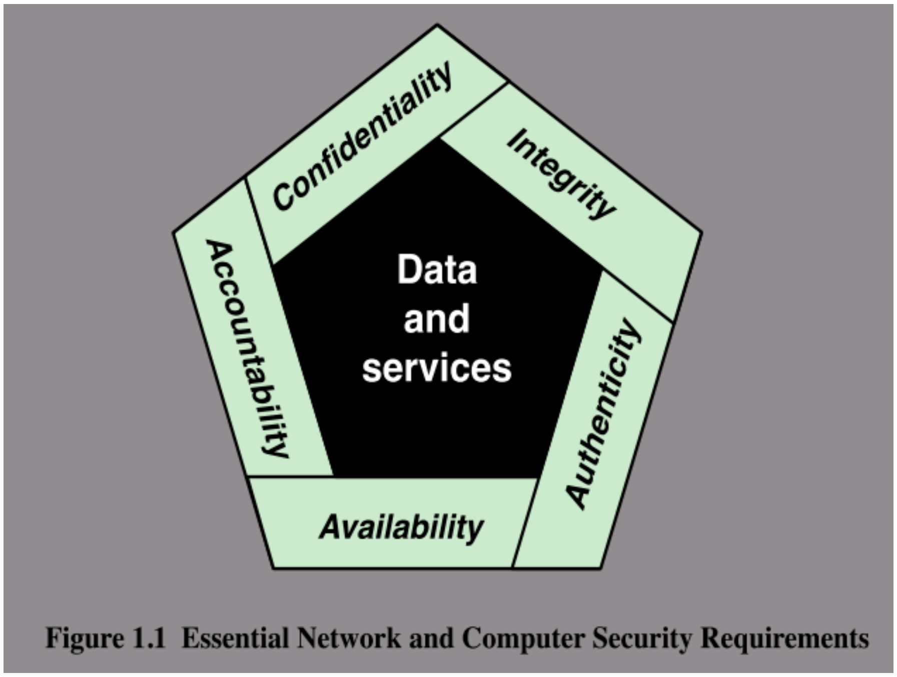


Figure 1.1 Essential Network and Computer Security Requirements

- **Authenticity**: This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. Ways to achieve accountability are: Access control, Auditing and logging, Identity and Access Management.

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. Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security
4. 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
5. Security requires regular and constant monitoring

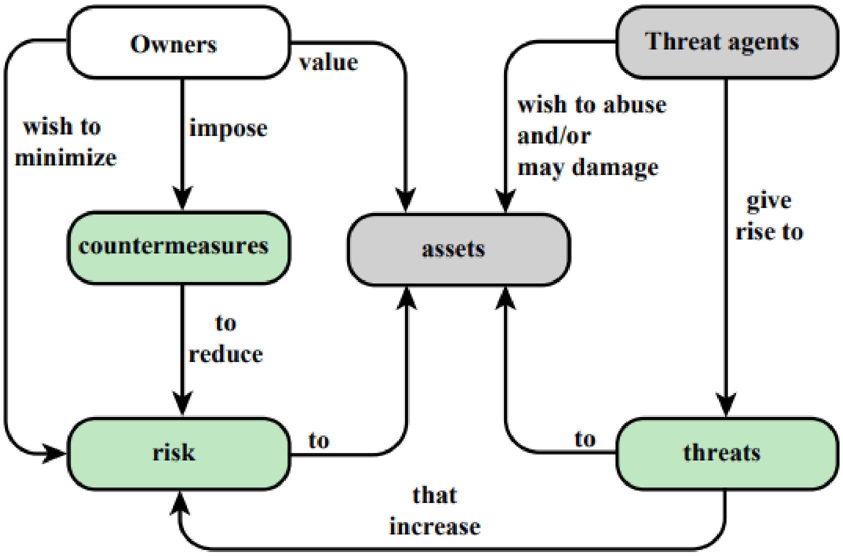
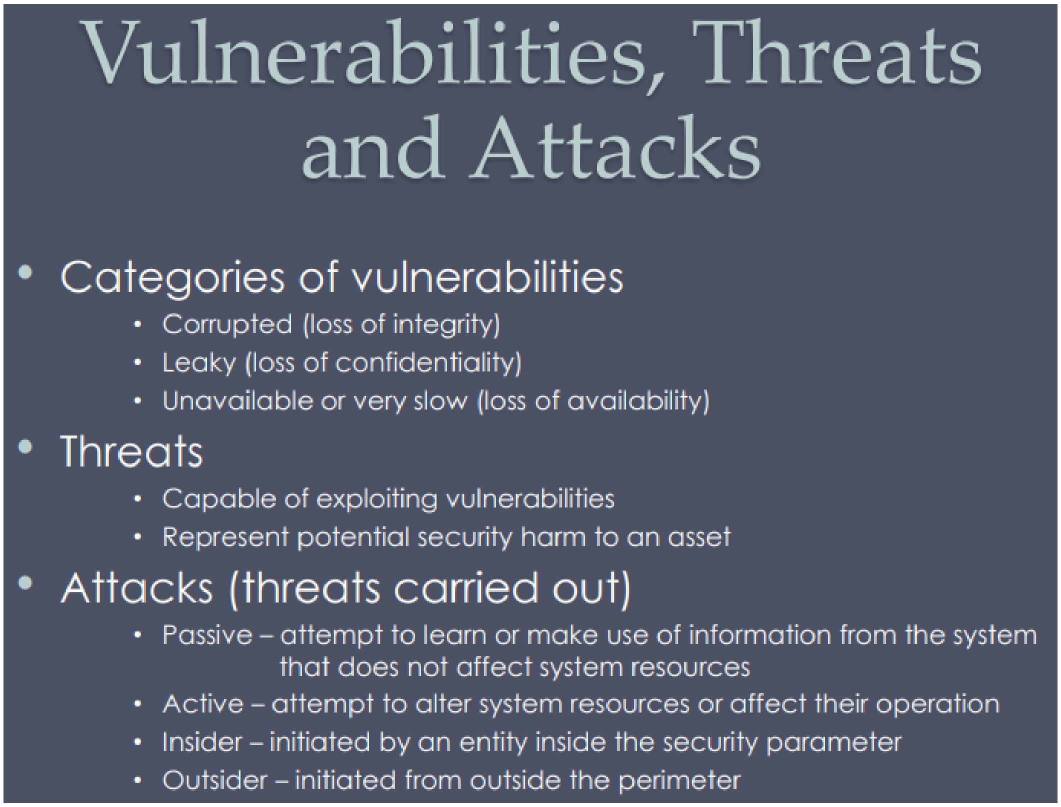
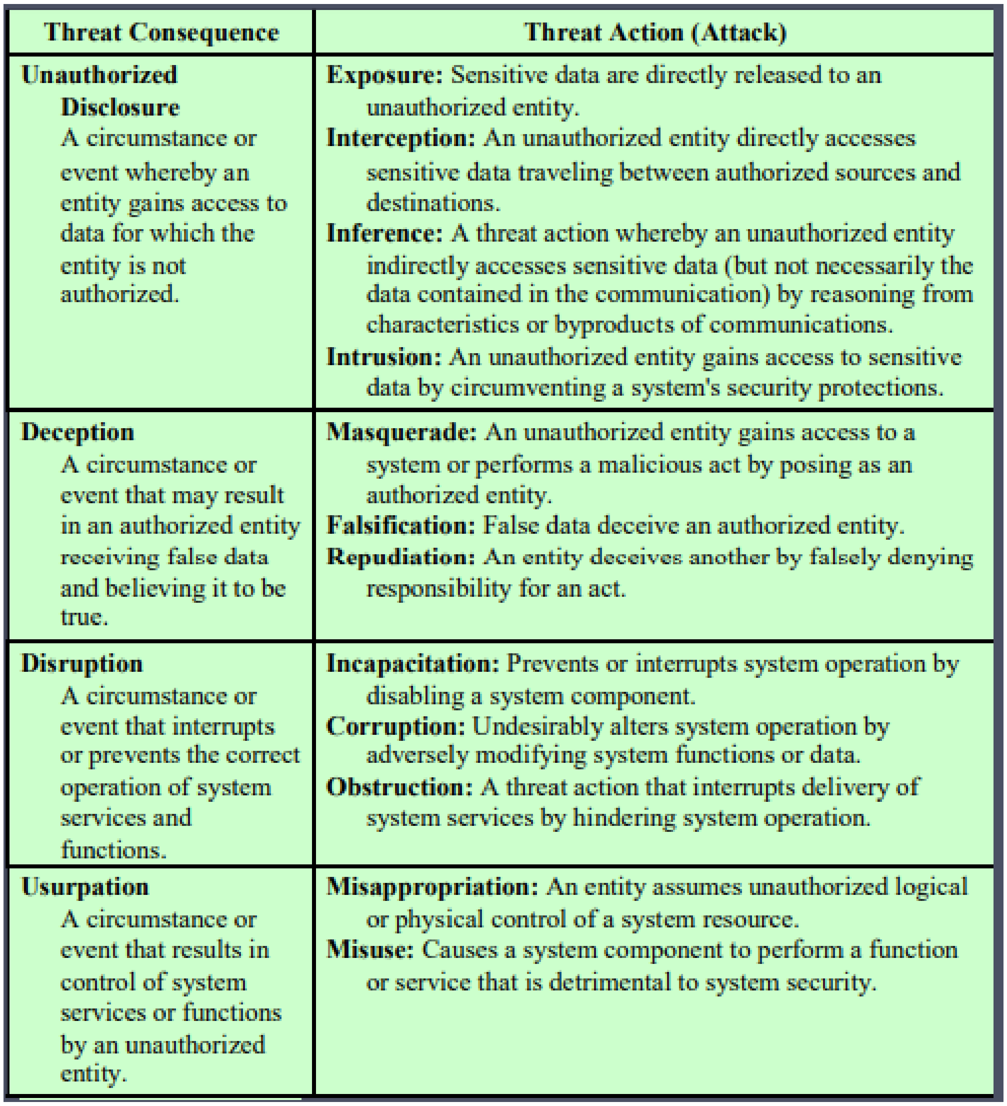


Figure 1.2 Security Concepts and Relationships



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



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.

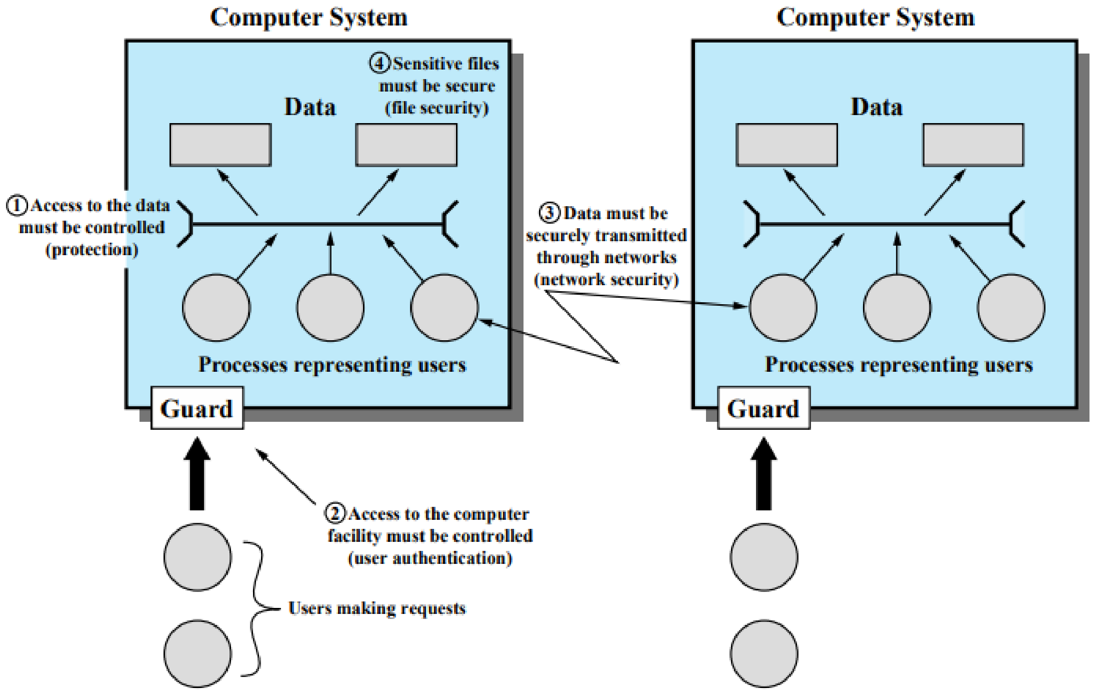
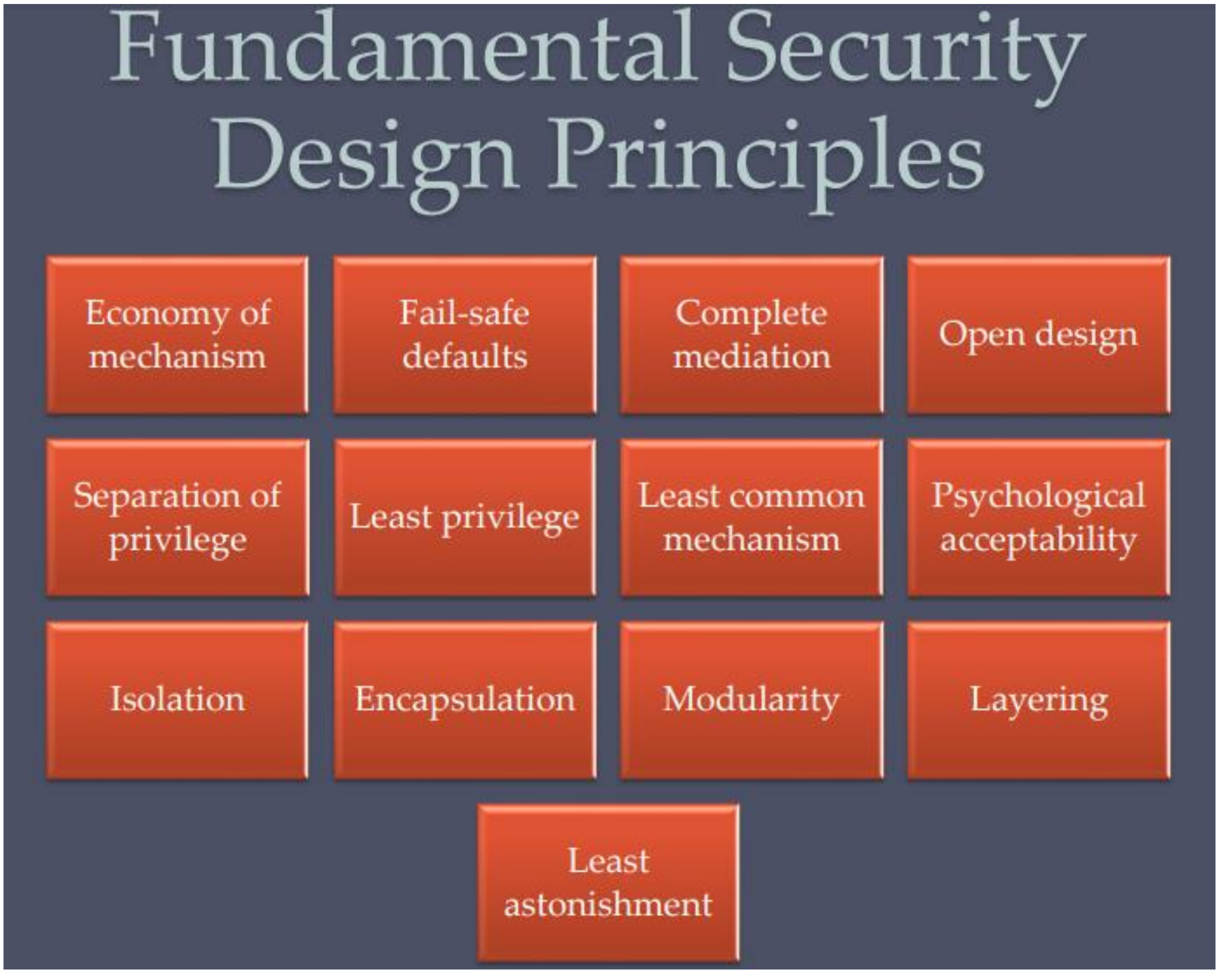
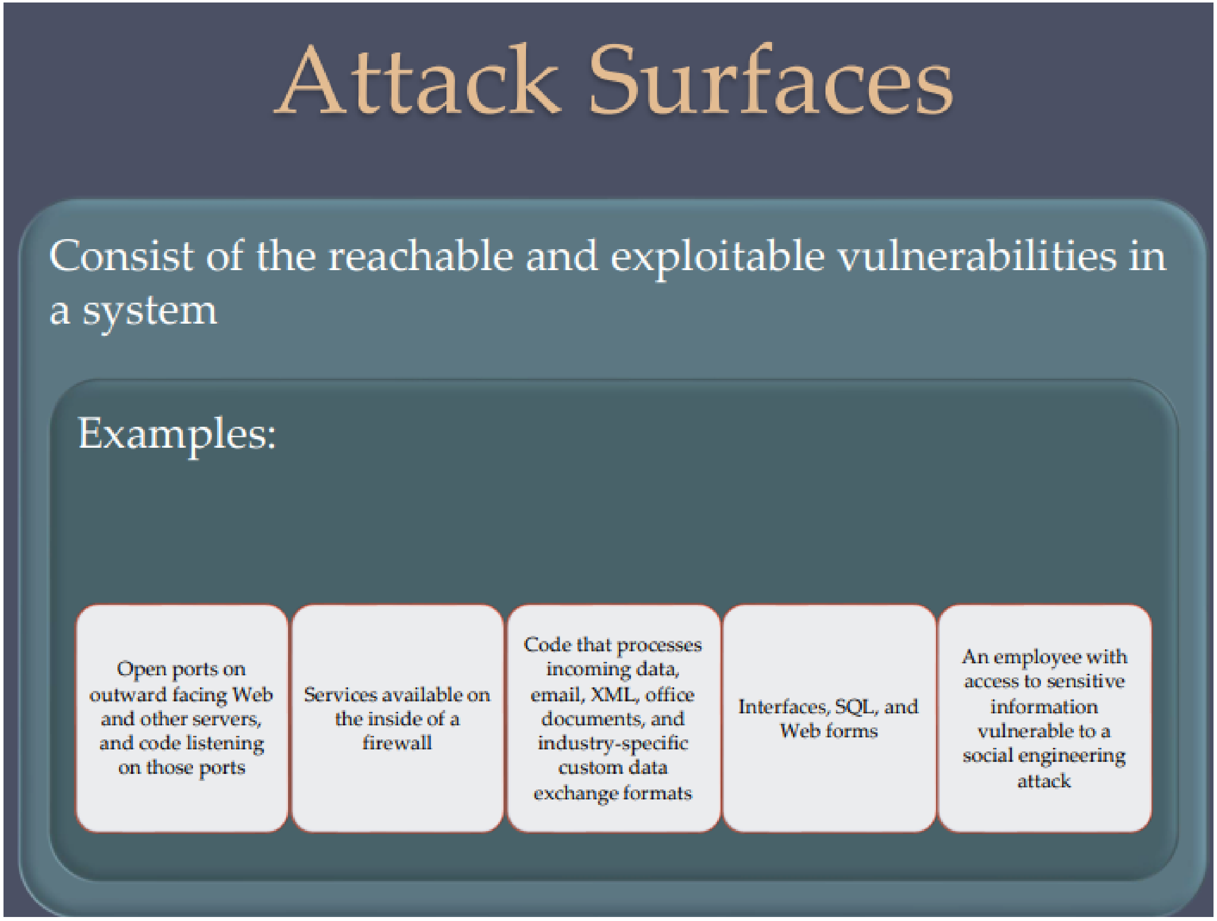

Computer System
Computer System
④Sensitive files must be secure (file security)
Data
Data
①Access to the data must be controlled (protection)
③Data must be securely transmitted through networks (network security)
Processes representing users
Processes representing users
Guard
Guard
②Access to the computer facility must be controlled (user authentication)
Users making requests

Figure 1.3 Scope of Computer Security. This figure depicts security



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

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:

1. National Institute of Standards and Technology - NIST
2. Internet Society - ISOC
3. International Telecommunication Union - ITU-T
4. International Organization for Standardization - ISO