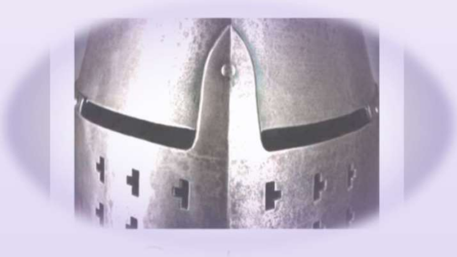


Chapter 1

Computer and Network Security Concepts

Cybersecurity

- A collection of tools, policies, security concepts, security guidelines, risk management, approaches, … , that are used to protect cyberspace environment and assets of users
- User assets
  - Computing devices
  - Applications
  - Communication
  - Personal information
  - Data
  - …

Cybersecurity categories

- Information security
  - Preserve confidentiality, integrity and availability of information
  - Other objectives: authenticity, accountability, nonrepudiation, reliability, …
- Network security
  - Protect networks and their services from unauthorized modification, destruction or disclosure
  - Assure to perform critical functions correctly and no harmful side effects

Cybersecurity objectives

- Confidentiality
  - Data confidentiality: assure that private or confidential information is not made available or disclosed to unauthorized individuals
  - Privacy: assure 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
  - Data integrity: assure that data and programs are changed only in a specified and authorized manner
  - System integrity: assure that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

- Availability
  - Assure that systems work promptly and service is not denied to authorized users
- Non-repudiation
  - One cannot deny what he has done, such as, deny the message sent by him thru a network
- Authenticity
- Accountability
- …

Computer security challenges

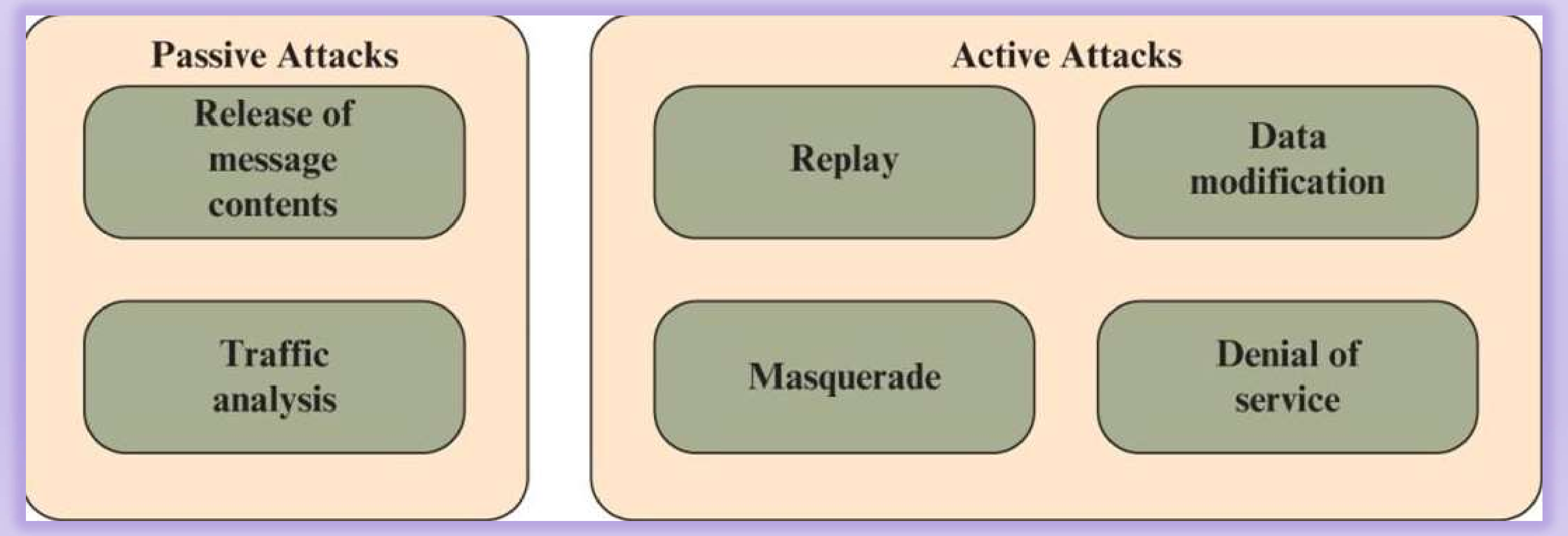
- Not as simple as it appears to be
- Potential attacks are hard to find
- Protective procedures are often counter-intuitive
- Need constant monitoring
- Too often as afterthought
- Security mechanisms are often complicated
- Unaware until a security failure occurs
- Strong security are often viewed as impediment to efficient and user-friendly operation
- …

OSI security architecture

- Security attack
  - Any action that compromises security of information and system
- Security mechanism
  - A process that is designed to detect, prevent, or recover from security attacks
- Security service
  - A processing or communication service that enhances security of data processing systems and information transfers
  - Security mechanisms provide services for countering security attacks

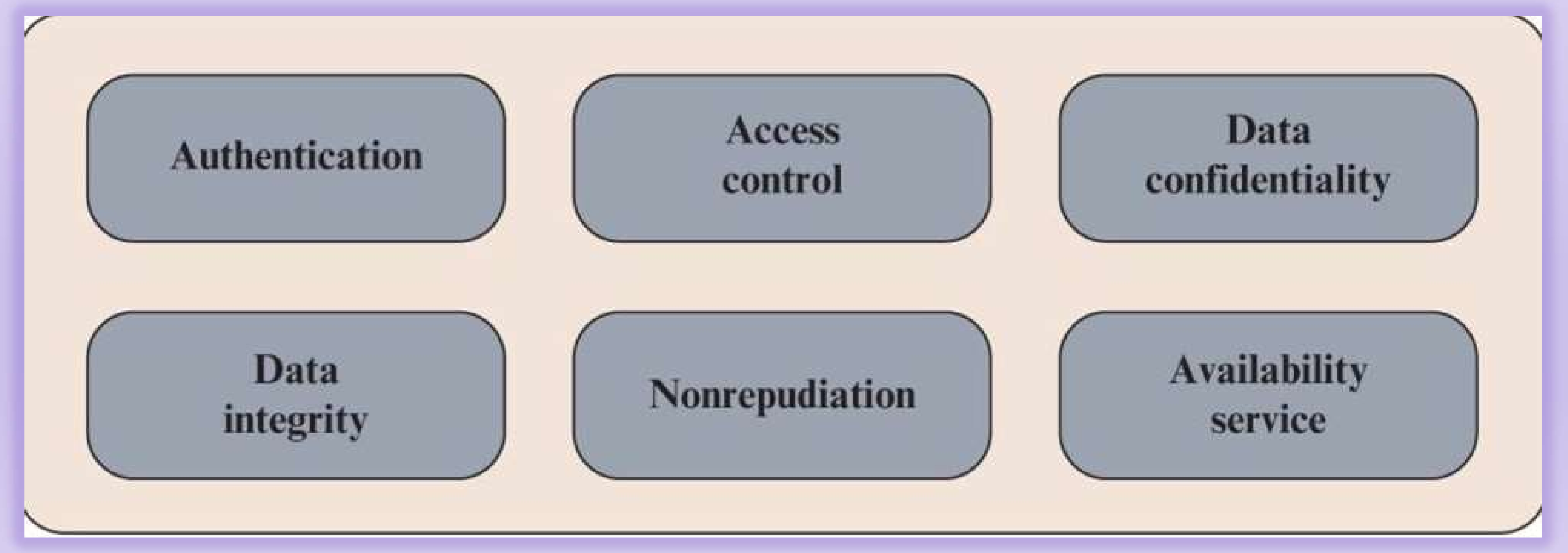
Security concept: attacks

- Threat: circumstance or event with potential impact on security of information and system
- Attack: malicious activity that attempts to compromise security of information and system
- Types



Security concept: services

- Security service is a capability that supports one or more security requirements
- Security service implements security policies
- Security service is implemented by security mechanism
- Types



Authentication

Access control

Data confidentiality

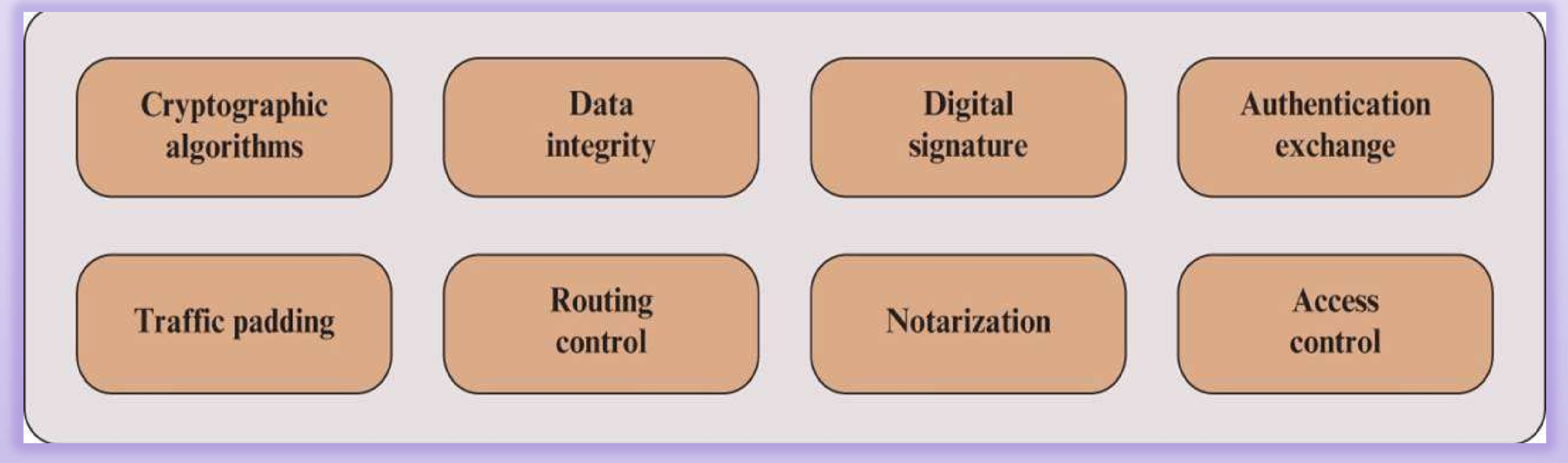
Data integrity

Nonrepudiation

Availability service

Security concept: mechanism

- Methods that supports security services
- Types



Cryptographic algorithms

Data integrity

Digital signature

Authentication exchange

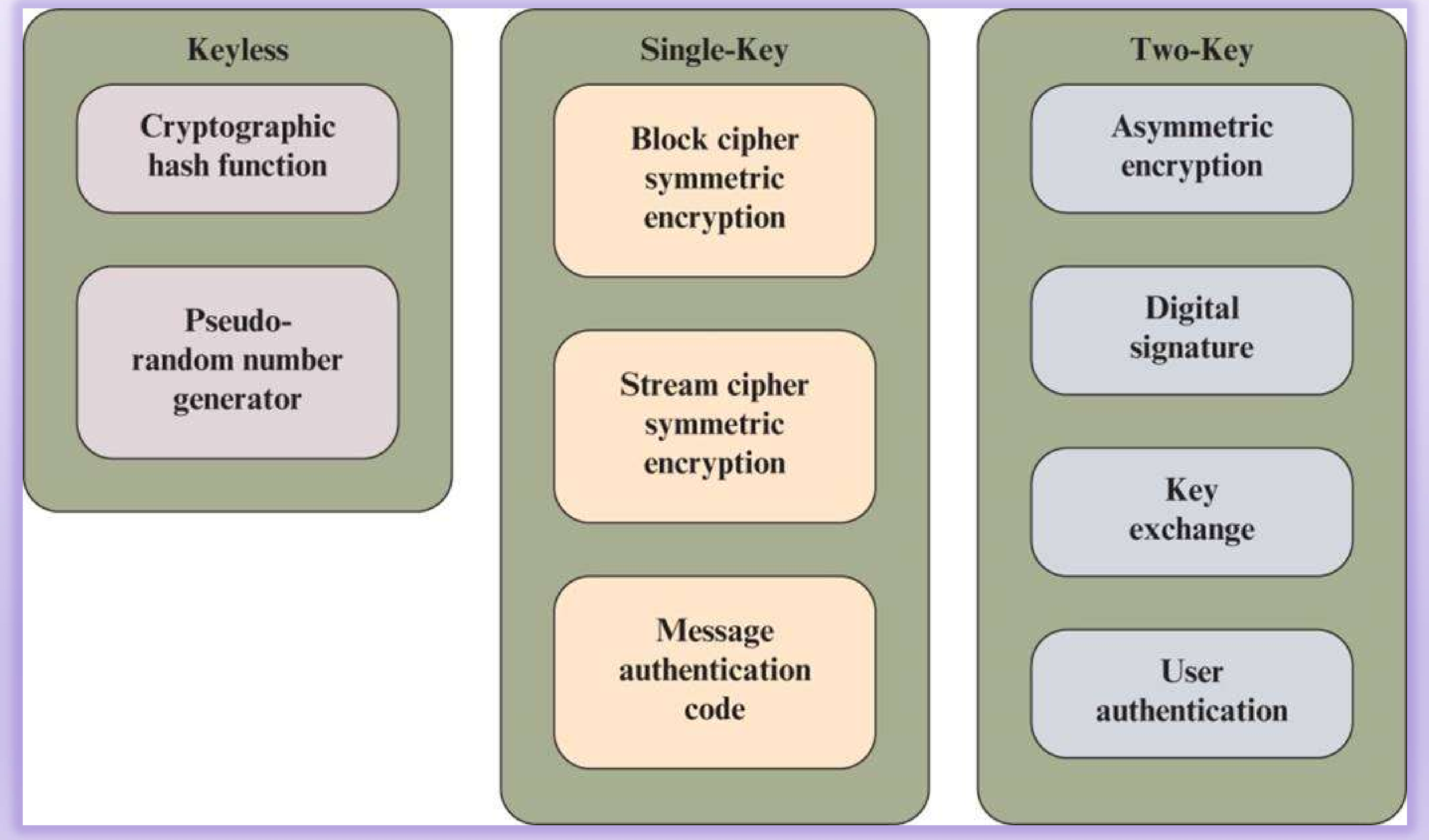
Traffic padding

Routing control

Notarization

Access control

Cryptographic algorithms



Keyless

- Cryptographic hash function
- Pseudo-random number generator

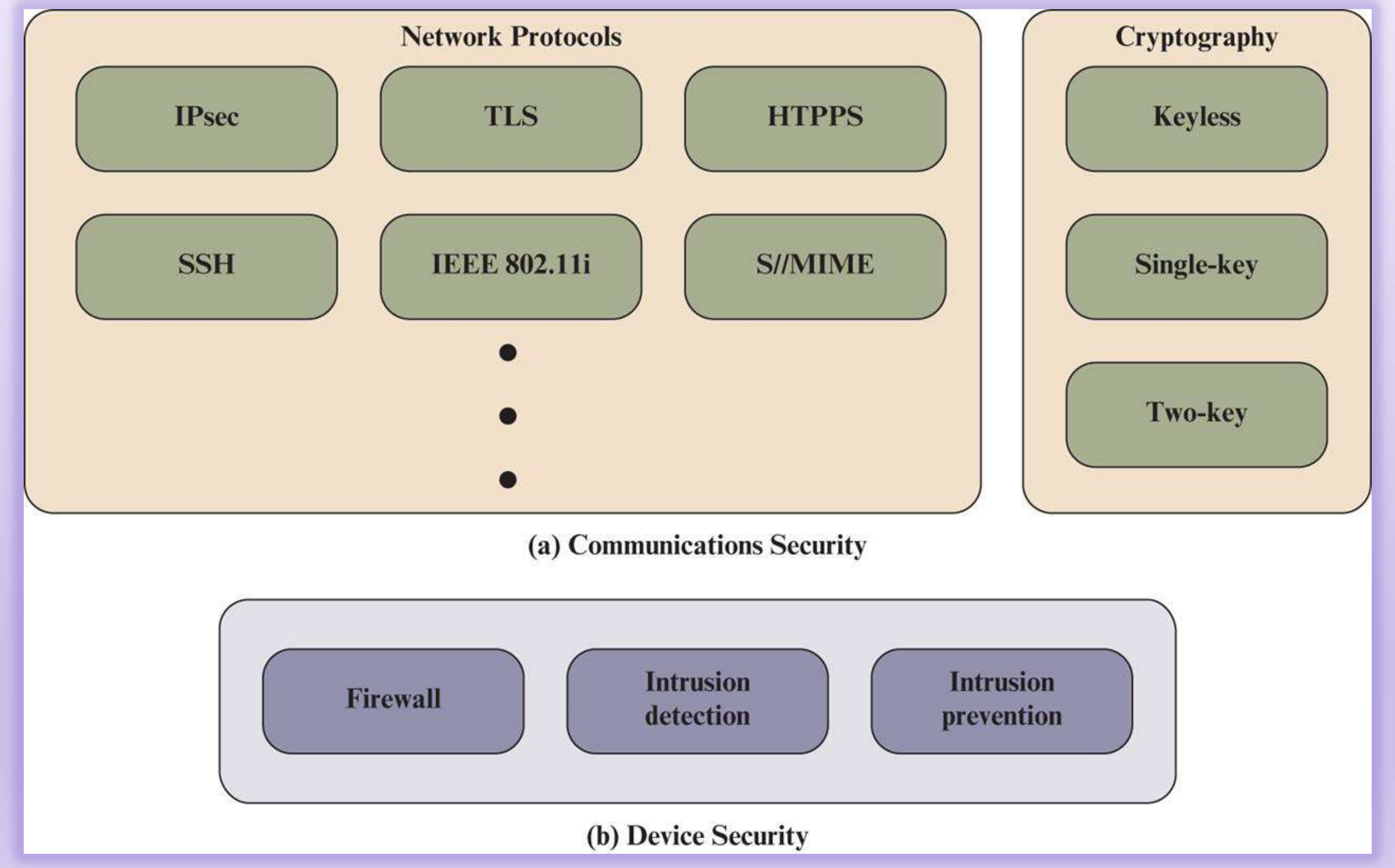
Single-Key

- Block cipher symmetric encryption
- Stream cipher symmetric encryption
- Message authentication code

Two-Key

- Asymmetric encryption
- Digital signature
- Key exchange
- User authentication

Network security: key elements



Security design principles

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

Standards

- NIST: National Institute of Standards and Technology:
  - A U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government
  - Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact
- Internet Society
  - ISOC is a professional society that provides leadership in addressing related issues, such as, Internet infrastructure standards,
  - Internet Engineering Task Force (IETF) : develop Internet standards and related specifications, published as Requests for Comments (RFC).

- ITU- International Telecommunication Union
  - An international organization under United Nations
  - ITU-T (Telecommunication Standardization Sector): to develop technical standards for communications. Its standards are referred as Recommendations
- ISO: International Organization for Standardization
  - A worldwide federation of national standards bodies from more than 140 countries
  - A nongovernmental organization that promotes the development of standardization and related activities
  - Its standards are referred as International Standards ISO