The OSI Security Architecture

IT3122 Computer Security

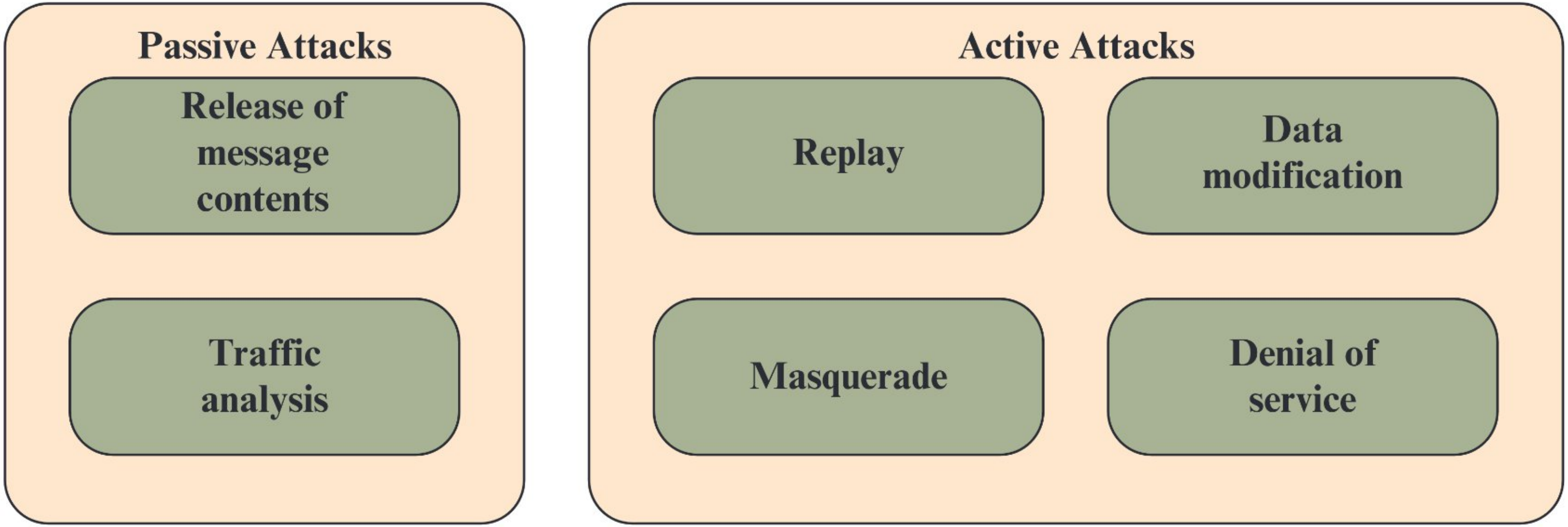
Intended Learning Outcomes

- Discuss the types of security threats and attacks that must be dealt with and give examples of the types of threats and attacks that apply to different categories of computer and network assets.
- List security controls.
- Provide an overview of the main areas of network security.

The OSI Security Architecture

- **Security attack**: Any action that compromises the security of information owned by an organization.
- **Security mechanism**: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

Attacks


Passive Attacks
Release of message contents
Traffic analysis
Active Attacks
Replay
Data modification
Masquerade
Denial of service

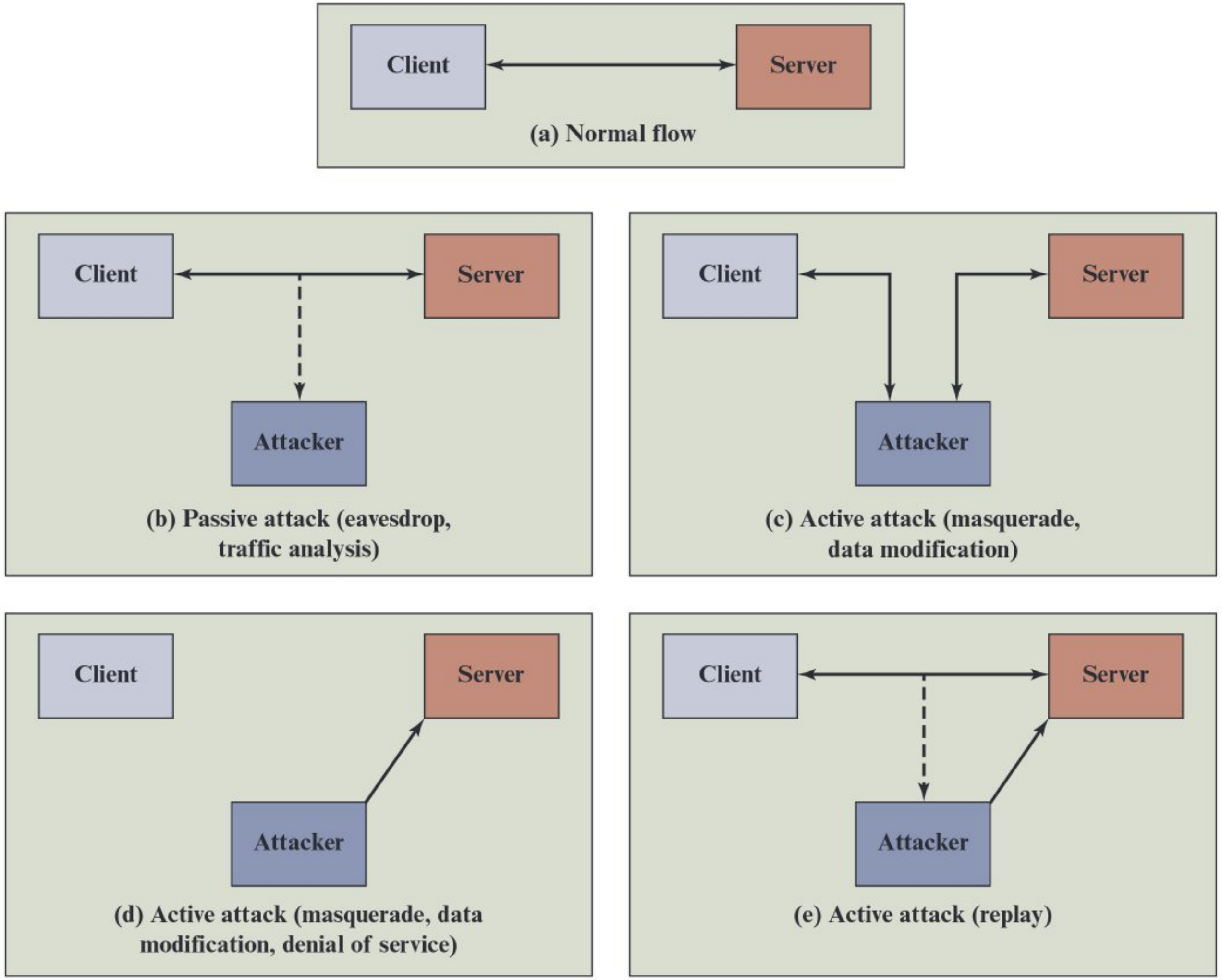
Passive Attacks

- **Passive attacks** are in the nature of **eavesdropping** on, or monitoring of, transmissions.
- The **release of message contents** is learning the contents of the transmissions.
- **Traffic analysis** is observing the pattern of the messages.

Active Attacks

- **Active attacks** involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:
  1. A **masquerade** takes place when one entity pretends to be a different entity.
  2. **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
  3. **Data modification** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
  4. The **denial of service** prevents or inhibits the normal use or management of communication facilities.

Security Attacks



(a) Normal flow

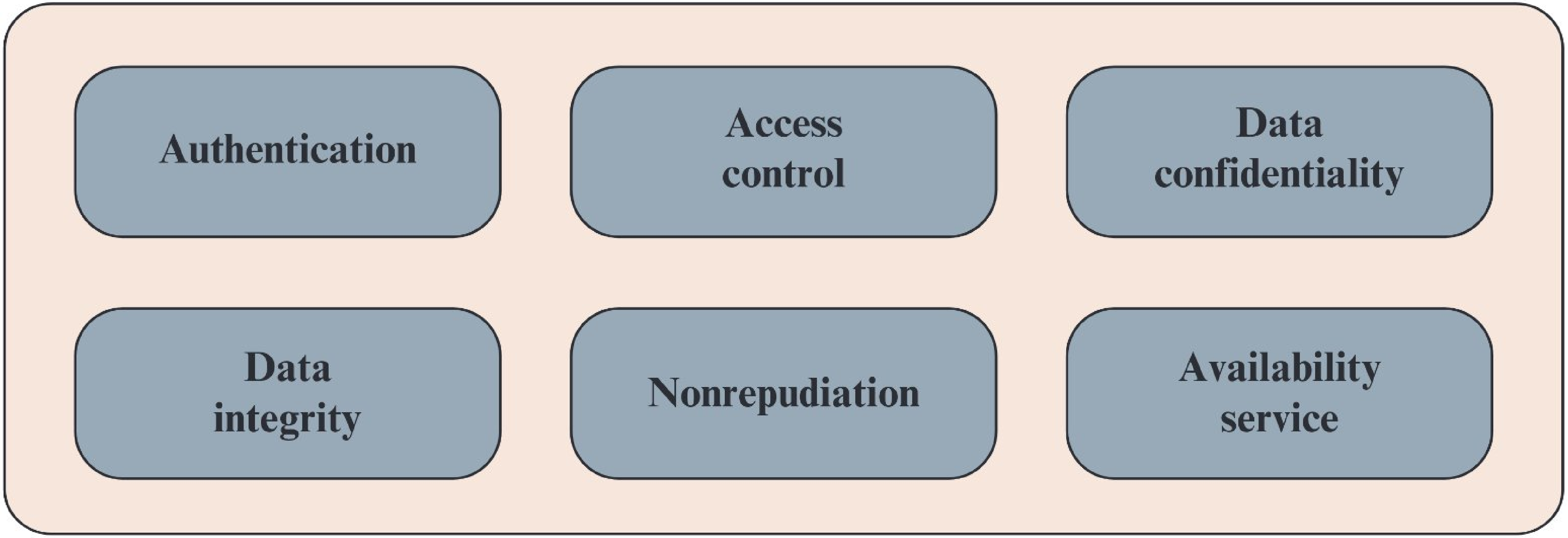
(b) Passive attack (eavesdrop, traffic analysis)

(c) Active attack (masquerade, data modification)

(d) Active attack (masquerade, data modification, denial of service)

(e) Active attack (replay)

Services



Authentication

Access control

Data confidentiality

Data integrity

Nonrepudiation

Availability service

Authentication

- The **authentication** service is concerned with assuring that a communication is authentic.
- Two specific authentication services are defined in X.800:
    1. **Peer entity authentication**: Provides for the corroboration of the identity of a peer entity in an association.
    2. **Data origin authentication**: Provides for the corroboration of the source of a data unit.

Access Control

- In the context of network security, **access control** is the ability to limit and control the access to host systems and applications via communications links.

Data Confidentiality

- **Confidentiality** is the protection of transmitted data from passive attack.

Data Integrity

- A **connection-oriented integrity** service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.
- A **connectionless integrity** service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.

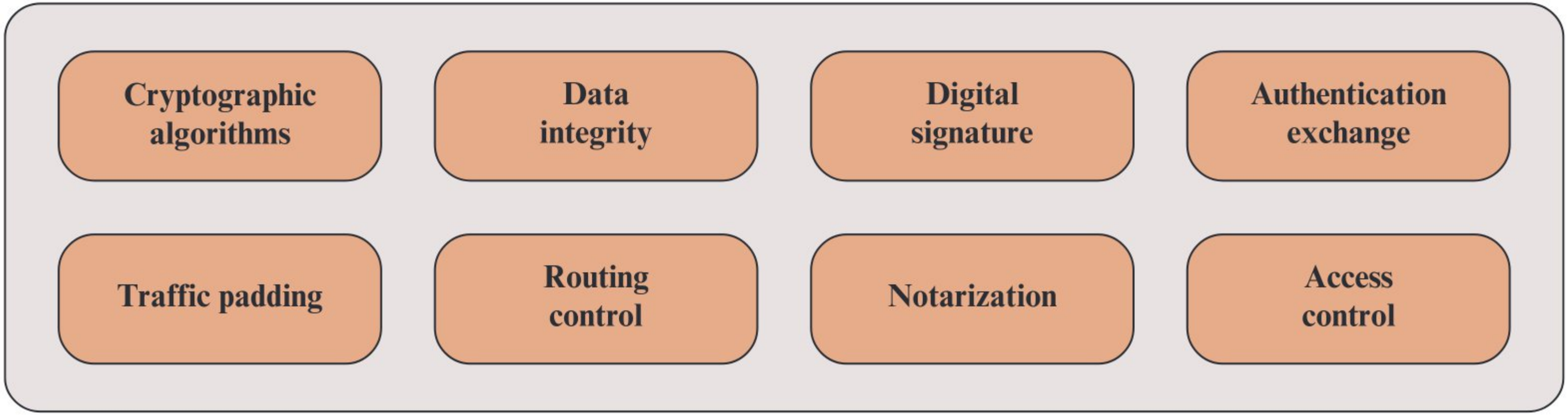
Nonrepudiation

- Nonrepudiation prevents either sender or receiver from denying a transmitted message.

Availability Service

- **Availability** is the property of a system, or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.

Mechanisms



Cryptographic algorithms

Data integrity

Digital signature

Authentication exchange

Traffic padding

Routing control

Notarization

Access control

Security Mechanisms

- **Cryptographic algorithms**: A **reversible cryptographic mechanism** is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. **Irreversible cryptographic mechanisms** include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.
- **Data integrity**: This category covers a variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Security Mechanisms

- **Digital signature**: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.
- **Authentication exchange**: A mechanism intended to ensure the identity of an entity by means of information exchange.
- **Traffic padding**: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Security Mechanisms

- **Routing control**: Enables selection of particular physically or logically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- **Notarization**: The use of a trusted third party to assure certain properties of a data exchange.
- **Access control**: A variety of mechanisms that enforce access rights to resources.

Security Control

- A **security control** is a safeguard or countermeasure an organization implements to help reduce risk.
- **Total risk** is the combined risk to all business assets.
- **Residual risk** is the risk that remains after countermeasures and controls have been deployed:

$$\text{Risk} - \text{Mitigating controls} = \text{Residual risk}$$

Activity Phase Controls

- Activity phase controls can be either administrative or technical.
- Some controls manage the activity phase of security, or the things people do, and are known as **administrative controls**.
- A control carried out or managed by a computer system is a **technical control**.

Activity Phase Controls

- **Detective controls**—These controls identify that a threat has landed in a system. E.g., intrusion detection system (IDS).
- **Preventive controls**—These controls stop threats from coming into contact with a vulnerability. E.g., intrusion prevention system (IPS).
- **Corrective controls**—These controls reduce the effects of a threat. E.g., reload an operating system after it is infected with malware.
- **Deterrent controls**—These controls deter an action that could result in a violation.
- **Compensating controls**—These controls are implemented to address a threat in place that does not have a straightforward risk-mitigating solution.

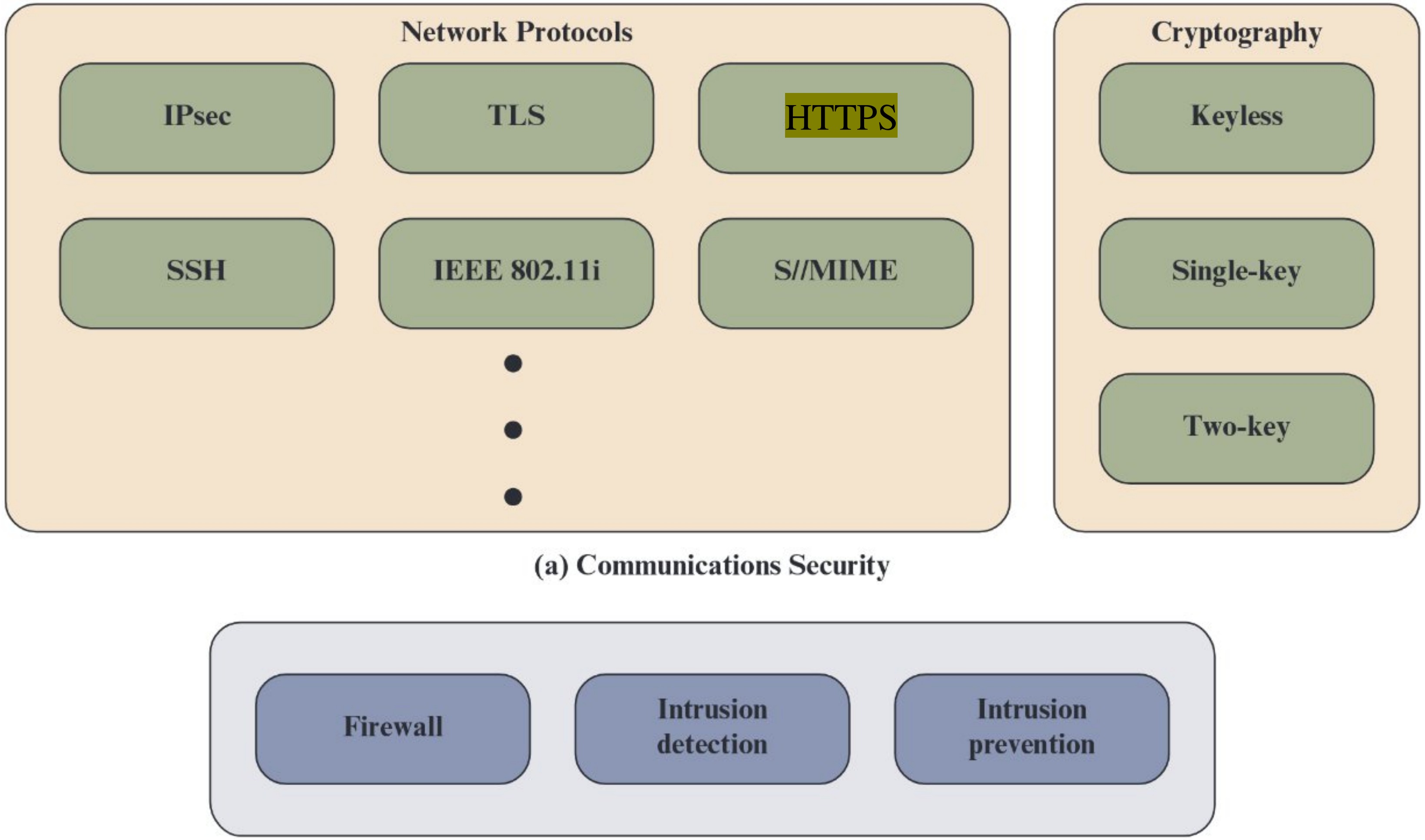
Environmental and Physical Controls

- Heating, ventilating, and air conditioning (HVAC)
- Fire suppression
- Electromagnetic interference (EMI) shielding
- Lighting
- Signs
- Fencing
- Barricades
- Guards
- Motion detectors

Environmental and Physical Controls

- Video surveillance
- Locks
- Mantraps
- Access lists
- Proximity readers
- Biometrics
- Protected access (cabling)
- Alarms

Key Elements of Network Security



(a) Communications Security

(b) Device Security

Network Security

1. **Communications security** deals with the protection of communications through the network, including measures to protect against both passive and active attacks.
2. **Device security** is the protection of network devices, such as routers and switches, and end systems connected to the network, such as client systems and servers.

Communications Security

- **Communications security** is primarily implemented using network protocols.
- A **network protocol** consists of the format and procedures that governs the transmitting and receiving of data between points in a network.
- One common characteristic of all of these protocols is that they use a number of **cryptographic** algorithms as part of the mechanism to provide security.

Device Security

1. **Firewall**: A hardware and/or software capability that limits access between a network and devices attached to the network, in accordance with a specific security policy.
2. **Intrusion detection**: Hardware or software products that gather and analyze information from various areas within a computer or a network for the purpose of finding, and providing real-time or near-real-time warning of, attempts to access system resources in an unauthorized manner.
3. **Intrusion prevention**: Hardware or software products designed to detect intrusive activity and attempt to stop the activity, ideally before it reaches its target.

References

- W. Stallings, “Information and Network Security Concepts,” in *Cryptography and Network Security, Principles and Practice*, 8th edition, 2023, pp. 21–43.
- D. Kim, and M. G. Solomon, “The Risk Management Process,” in *Fundamentals of Information Systems Security*, 4th edition, 2023, pp. 167–191.