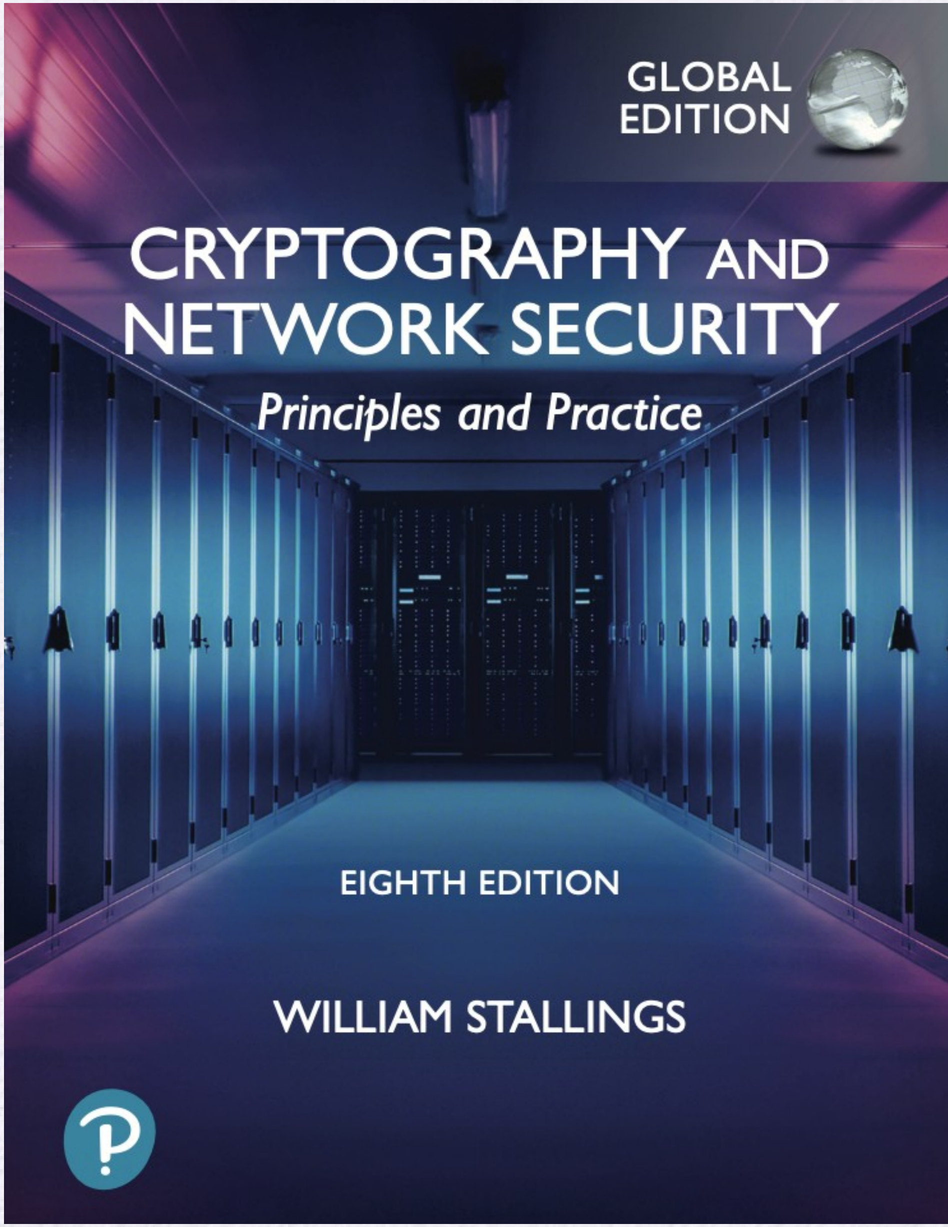
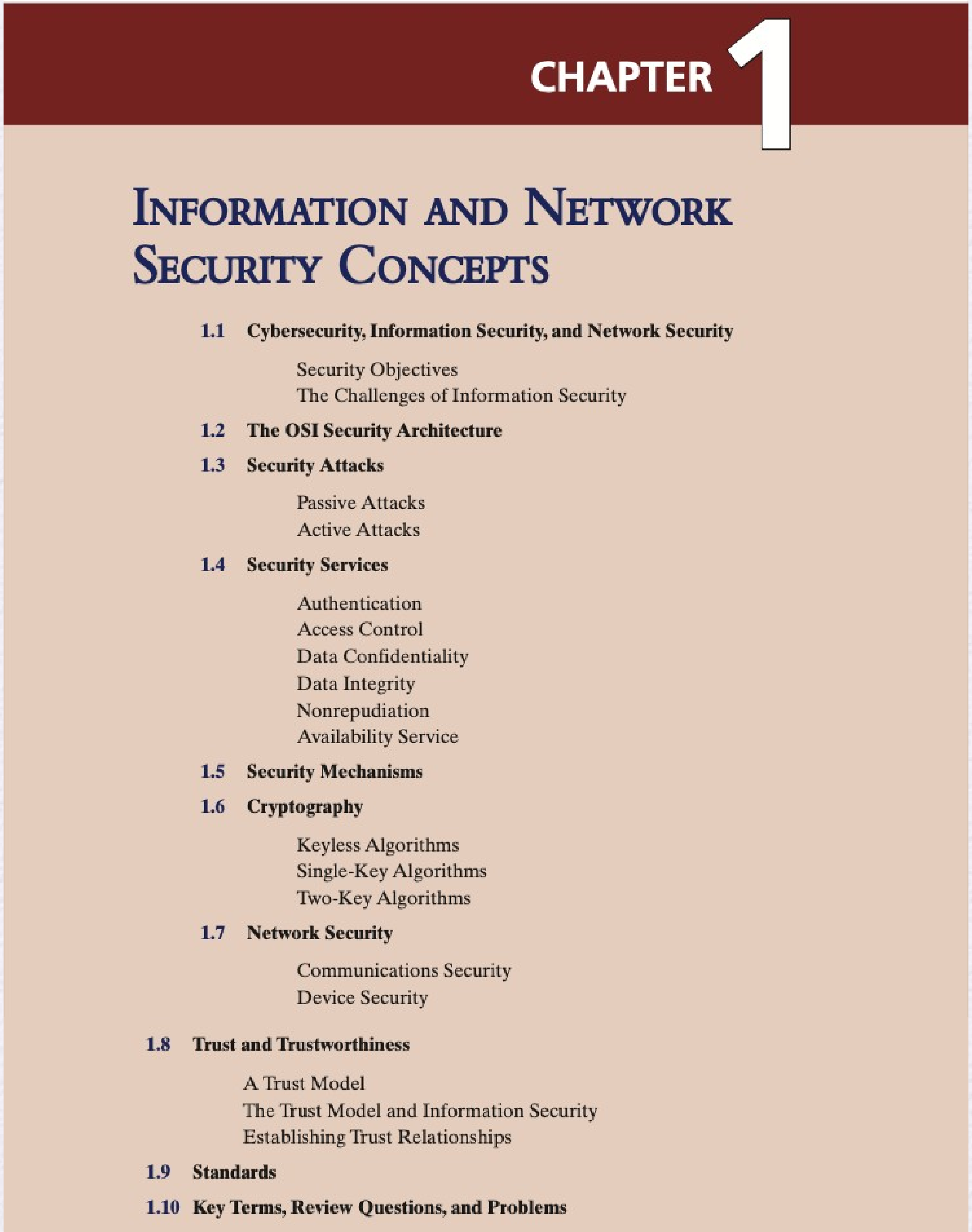
University of Nevada – Reno
Computer Science &
Engineering Department

CS454/654 Reliability and Security of Computing Systems - Fall 2024

Lecture 2

Dr. Batyr Charyyev
bcharyyev.com





CHAPTER 1

Information and Network Security Concepts

Cybersecurity

What is Cybersecurity?

Cybersecurity *is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyberspace environment and organization and users' assets.*

Organization and users' assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberspace environment.

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and users' assets against relevant security risks in the cyberspace environment. The general security objectives comprise the following: availability; integrity, which may include data authenticity, and confidentiality

Cybersecurity

As subsets of cybersecurity, we can define the following:

Information Security

- This term refers to preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved.

Network Security

- This term refers to protection of networks and their service from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects.

Q: What is Information and Network Security?

Security Objectives

- The cybersecurity definition introduces three key objectives that are at the heart of information and network security: Confidentiality, Integrity, Availability
    - **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

Q: What is Confidentiality, Integrity, Availability?

Security Objectives

- **Integrity:** This term covers two related concepts:
    - **Data integrity:** Assures that data and programs are changed only in a specified and authorized manner. This concept also encompasses data authenticity, which means that a digital object is indeed what it claims to be and nonrepudiation, which is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information
    - **System integrity**: Assures that a system performs its intended function, free from deliberate or planned unauthorized manipulation of the system
- **Availability:** Assures that systems work promptly and service is not denied to authorized users.

NIST standard FIPS 199 lists confidentiality, integrity, and availability as the three security objectives for information and for information systems.

- NIST: National Institute of Standards and Technology
- FIPS: Standards for Security Categorization of Federal Information and Information Systems

Authenticity: means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability: being able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches.

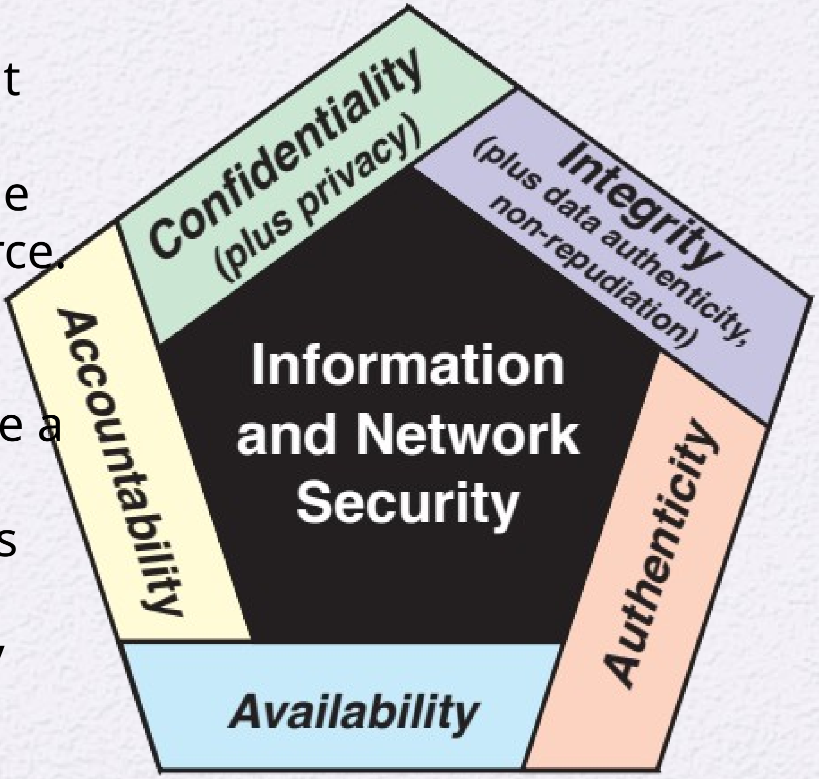


Figure 1.1 Essential Information and Network Security Objectives

Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered in designing system
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought

- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

Threats and Attacks

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

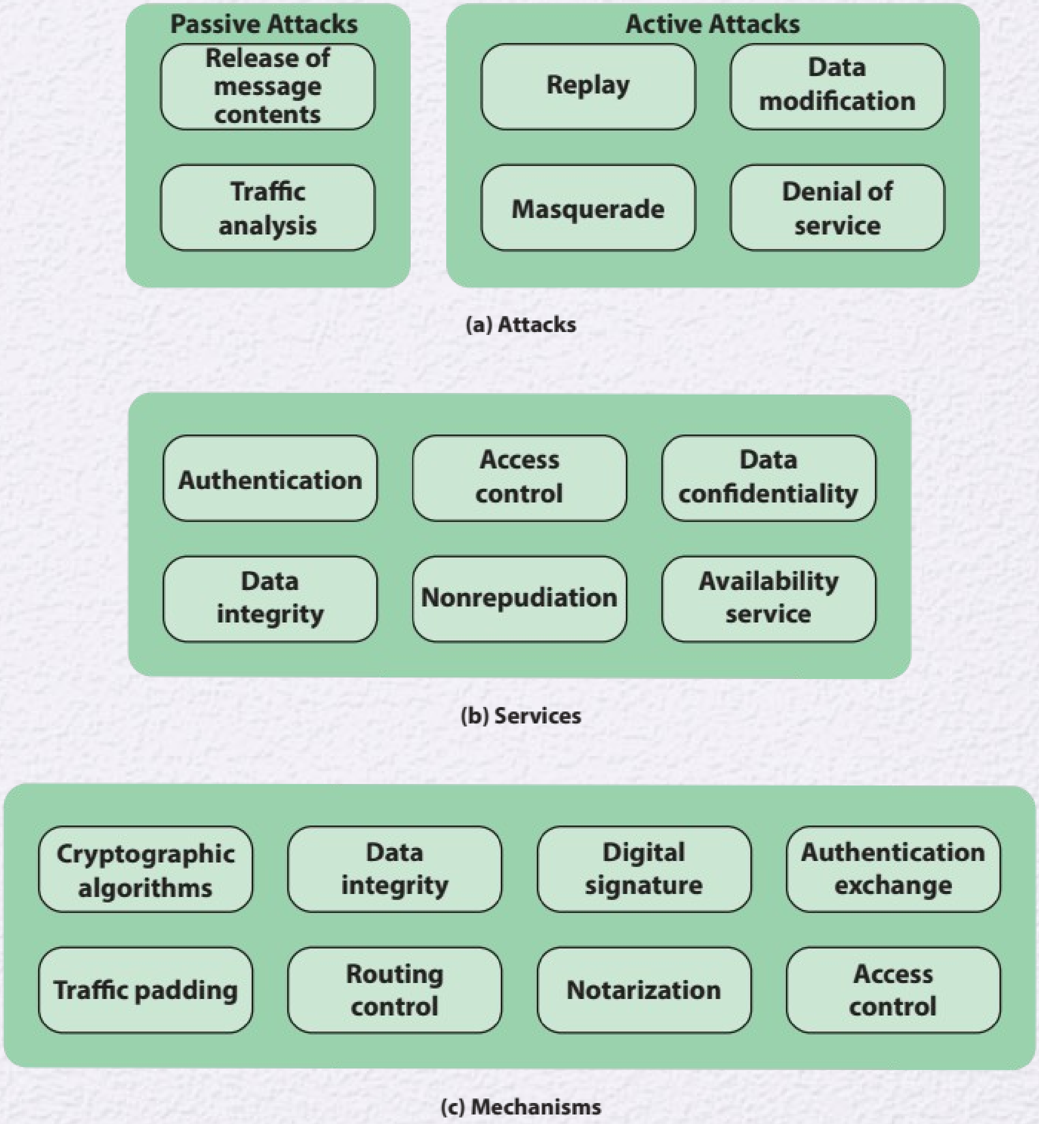
Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

- Security Attacks divided into two Passive and Active attacks.

- A security service is a capability that supports one or more of the security requirements (confidentiality, integrity, availability, authenticity, and accountability).

- Security services are implemented by security mechanisms.



Passive Attacks

Release of message contents

Traffic analysis

Active Attacks

Replay

Data modification

Masquerade

Denial of service

(a) Attacks

Authentication

Access control

Data confidentiality

Data integrity

Nonrepudiation

Availability service

(b) Services

Cryptographic algorithms

Data integrity

Digital signature

Authentication exchange

Traffic padding

Routing control

Notarization

Access control

(c) Mechanisms

Figure 1.2 Key Concepts in Security

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions.

- Goal of the opponent is to obtain information that is being transmitted.

- Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis

Active Attacks

- Involve some modification of the data stream or the creation of a false stream

- Goal is to detect attacks and to recover from any disruption or delays caused by them

Masquerade

- A masquerade takes place when one entity pretends to be a different entity.

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Data Modification

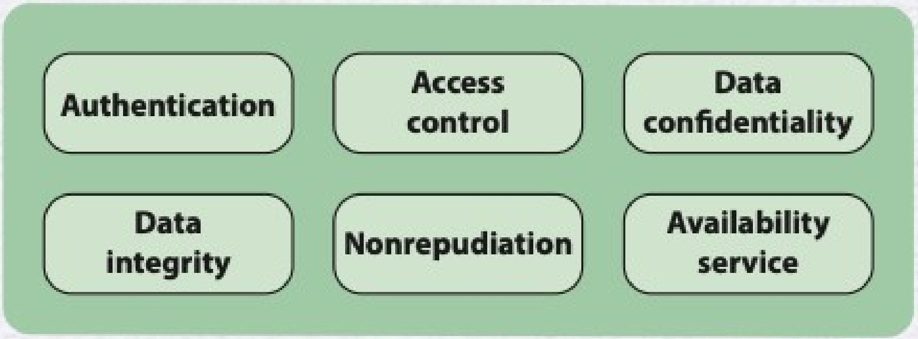
- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

Security services

Authentication



Authentication

Access control

Data confidentiality

Data integrity

Nonrepudiation

Availability service

(b) Services

- Concerned with assuring that a communication is authentic (real, original)
  - In the case of a single message, assures the recipient that the message is from the source that it claims to be from.
  - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties.

Authentication

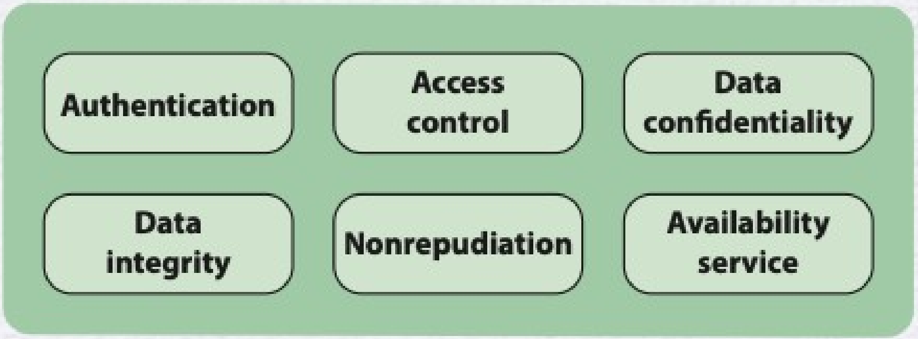
- **Two specific authentication services are defined in the field.**

- **Peer entity authentication**
  - The process of confirming identity of the entity. The goal is to ensure that the communicating system is genuine and not pretending to be another system or replaying a previous, unauthorized connection.

- **Data origin authentication**
  - The process of confirming the origin of a piece of data.

Access Control

Access control



Authentication

Access control

Data confidentiality

Data integrity

Nonrepudiation

Availability service

(b) Services

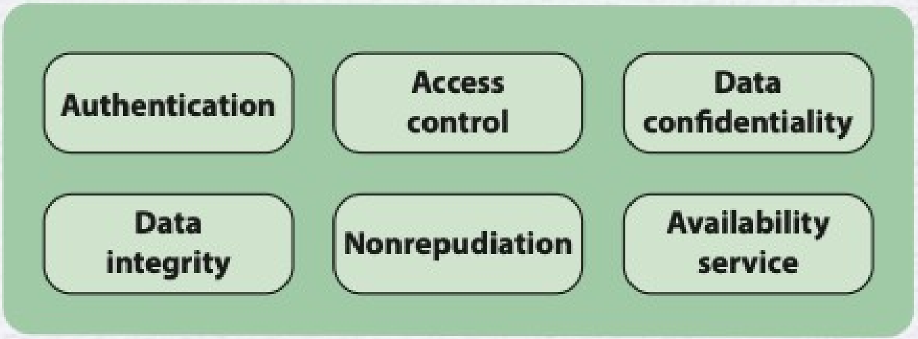
- The ability to limit and control the access to host systems and applications via communications links.

- To achieve this, each entity trying to gain access must first be indentified, or authenticated, so that access rights can be tailored to the individual.

Data Confidentiality, Integrity

Data Confidentiality

- The protection of transmitted data from passive attacks, and protection of traffic flow from analysis.
  - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility



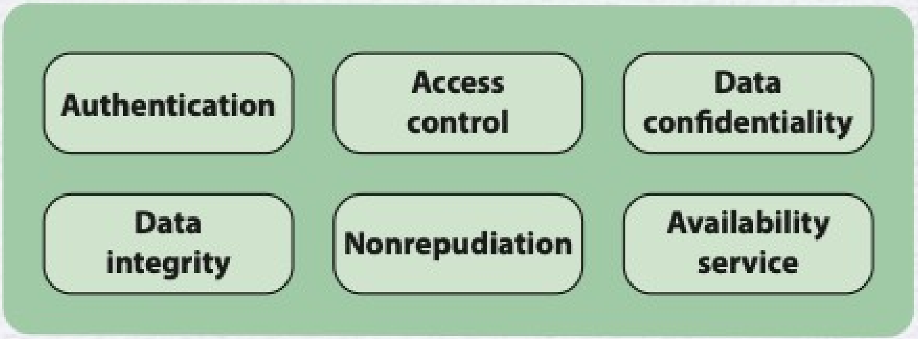
(b) Services

Data Integrity

- Assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.

Nonrepudiation

Nonrepudiation

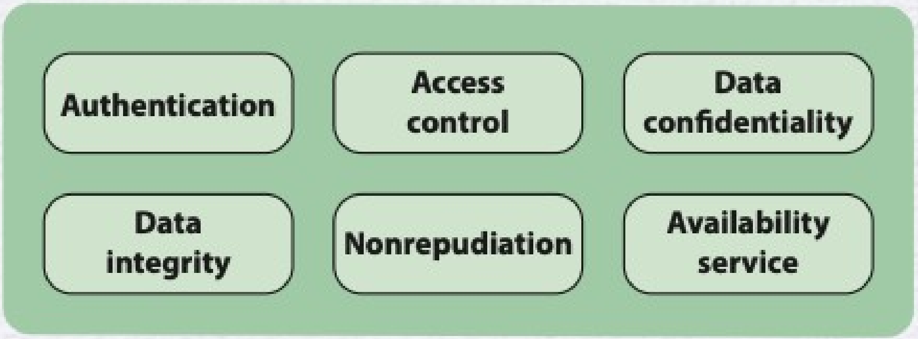


(b) Services

- Prevents either sender or receiver from denying a transmitted message.
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message.
- When a message is received, the sender can prove that the alleged receiver in fact received the message.

Availability Service

Availability

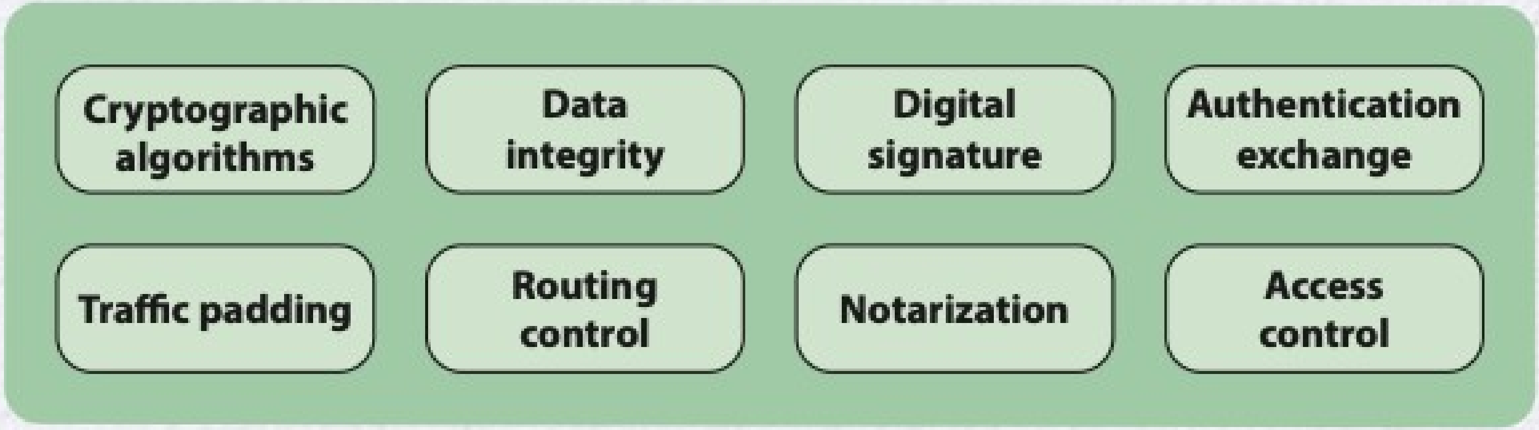


(b) Services

- Protects a system to ensure its availability
- This service addresses the security concerns raised by denial-of-service attacks
- It depends on proper management and control of system resources and thus depends on access control service and other security services.

Security Mechanisms

Most important security mechanisms discussed in this book



Cryptographic algorithms

Data integrity

Digital signature

Authentication exchange

Traffic padding

Routing control

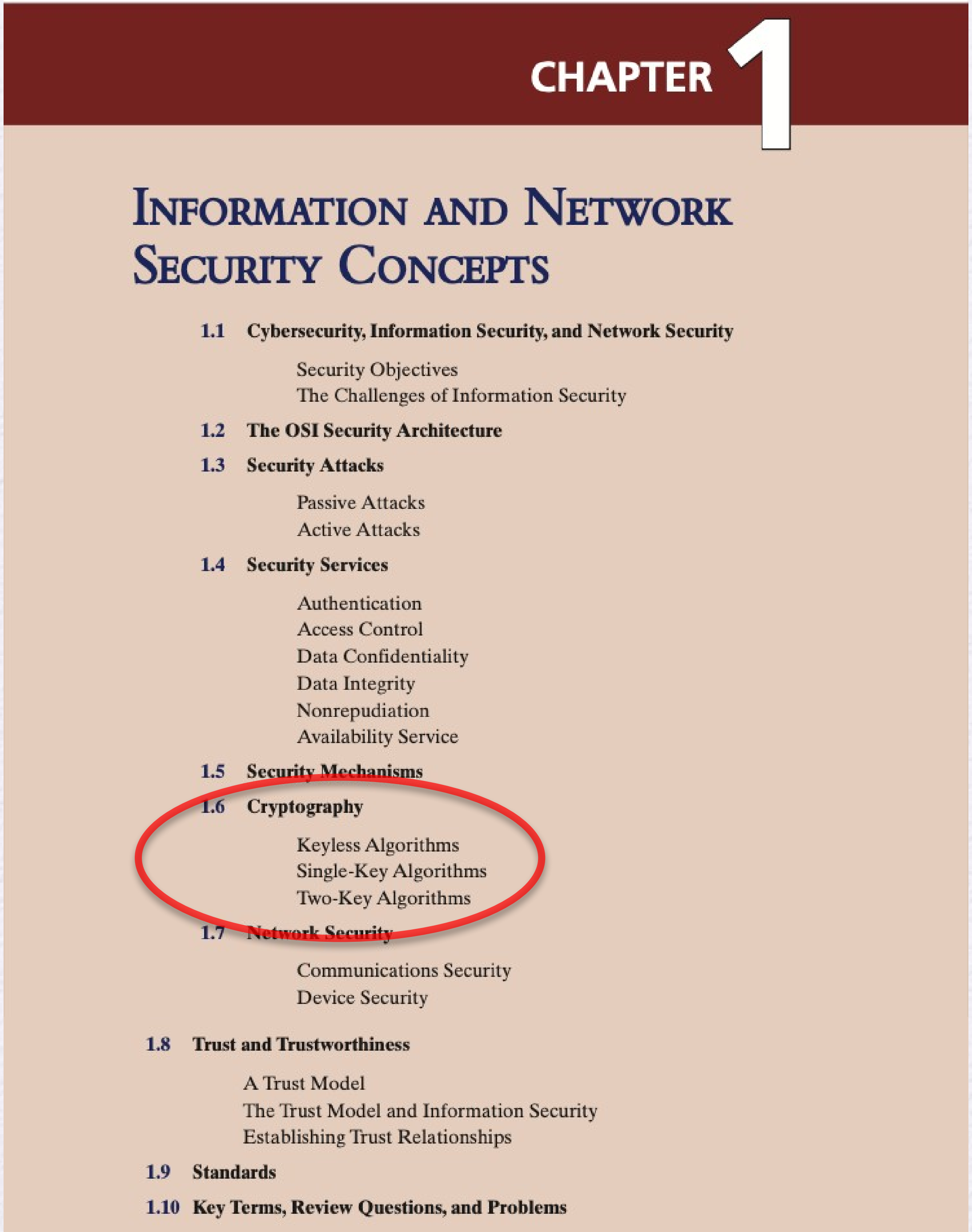
Notarization

Access control

(c) Mechanisms

Security Mechanisms

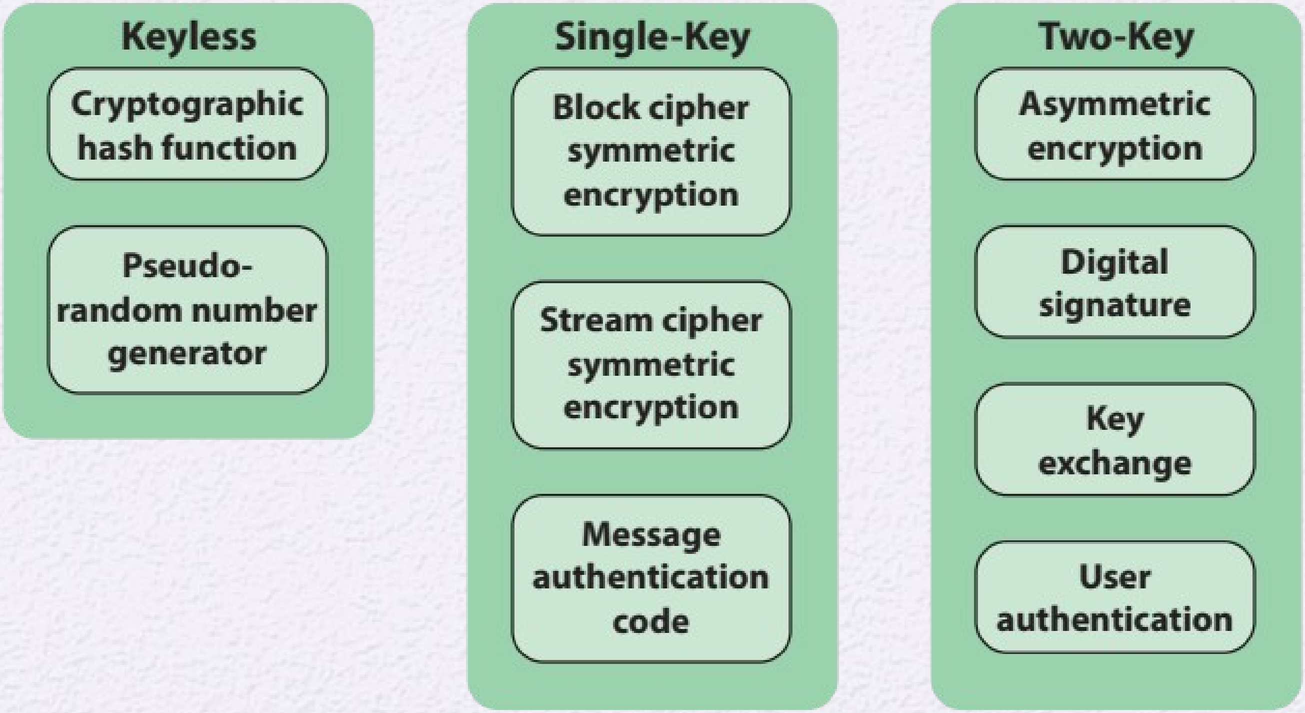
- **Cryptographic algorithms:** Two types reversible and irreversible cryptographic mechanisms. A reversible - encryption/decryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible - hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.
- **Data integrity:** This category covers a variety of mechanisms used to assure the integrity of a data.
- **Digital signature:** A digital signature is extra data added to a message or file that helps the receiver confirm who sent it and ensures it hasn't been tampered with.
- **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 prevent traffic analysis attempts.
- **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



CHAPTER 1

Information and Network Security Concepts

- **Keyless**: Do not use any keys during cryptographic transformations.
- **Single-key:** The result of a transformation is a function of the input data and a single key, known as a secret key.
- **Two-key:** At various stages of the calculation, two different but related keys are used, referred to as a private key and a public key.



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

Figure 1.4 Cryptographic Algorithms

Keyless Algorithms

- Deterministic functions that have certain properties useful for cryptography

- A cryptographic hash function turns a variable amount of text into a small, fixed-length value called a *hash value, hash code, or digest*
  - A *cryptographic hash function* is one that has additional properties that make it useful as part of another cryptographic algorithm, such as a message authentication code or a digital signature.

- A *pseudorandom number generator* produces a deterministic sequence of numbers or bits that has the appearance of being a truly random sequence.

Single-Key Algorithms

- Single-key cryptographic algorithms depend on the use of a secret key, shared by group of users.

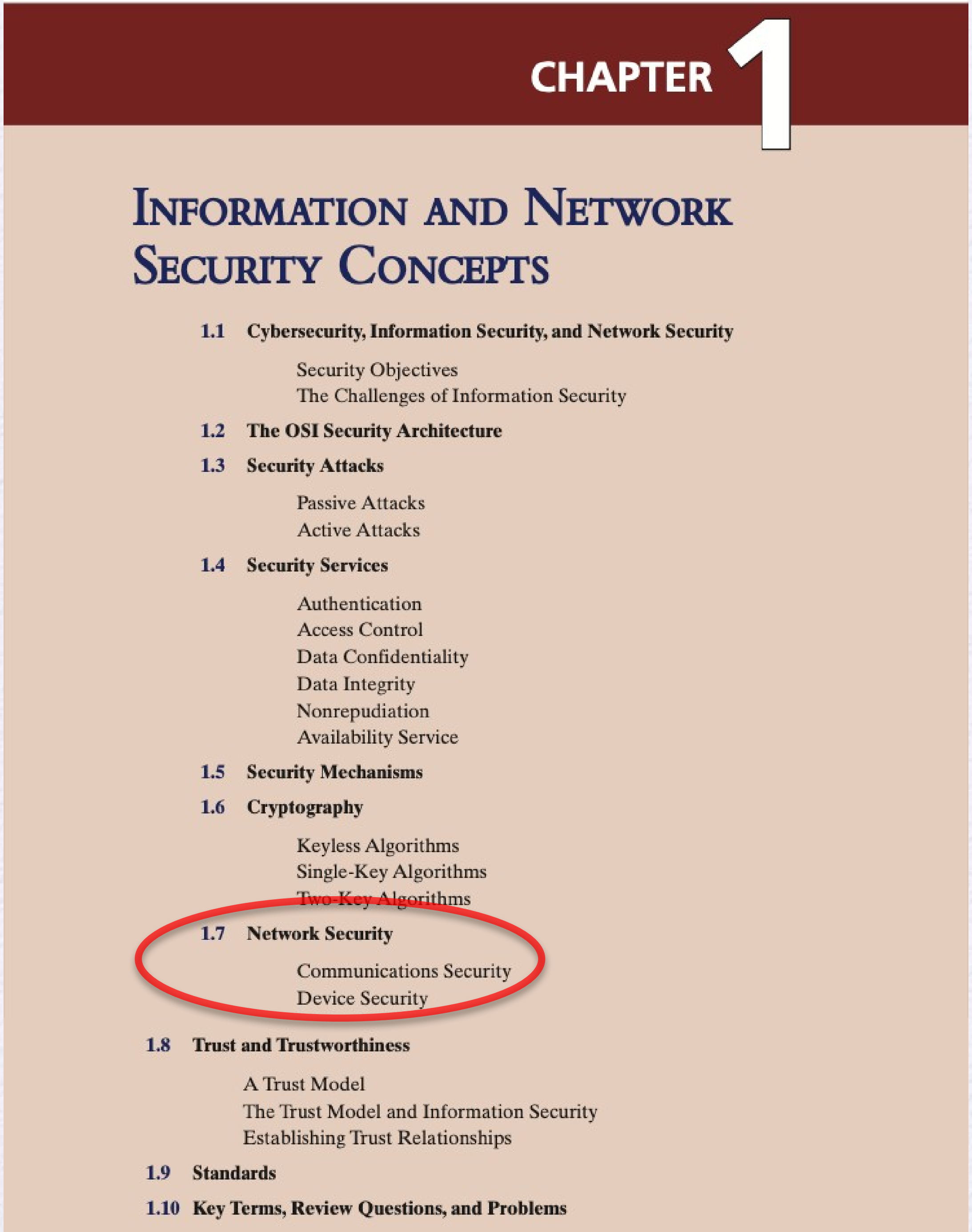
- Encryption algorithms that use a single key are referred to as symmetric encryption algorithms, takes two form:
  - **Block cipher:** A block cipher operates on data as a sequence of blocks.
    - A typical block size is 128 bits.
    - Depends not only on the current data block and the secret key but also on the content of preceding blocks.
  - **Stream cipher:** A stream cipher operates on data as a sequence of bits.
    - Typically, an exclusive-OR operation is used to produce a bit-by-bit transformation.

- Another form of single-key cryptographic algorithm is the message authentication code (MAC), used to verify the integrity of data.

Two-key Algorithms

- Encryption algorithms that use a two keys are referred to as *asymmetric encryption algorithms.* Keys referred as public and private keys.

- **Applications:** digital signature algorithm, key exchange, user authentication.
  - **Digital signature algorithm**: enables verify the data’s origin and integrity.
  - **Key exchange**: enables symmetric key distribution.
  - **User authentication**: enables the authentication process.



CHAPTER 1

Information and Network Security Concepts

Network Security

Network security is a broad term that encompasses security of the communications pathways of the network and the security of network devices and devices attached to the network

- **Communications Security:** deals with the protection of communications through the network, including measures to protect against both passive and active attacks
  - Implemented using network protocols, such as IPSec.
- **Device Security:** protection of network devices, such as routers and switches, and end systems connected to the network, such as client systems and servers.
  - The primary security concerns are intruders that gain access to the system to perform unauthorized actions, insert malicious software (malware), or overwhelm system resources to diminish availability.
  - Three types of device security are: **Firewall, Intrusion detection, Intrusion prevention.**

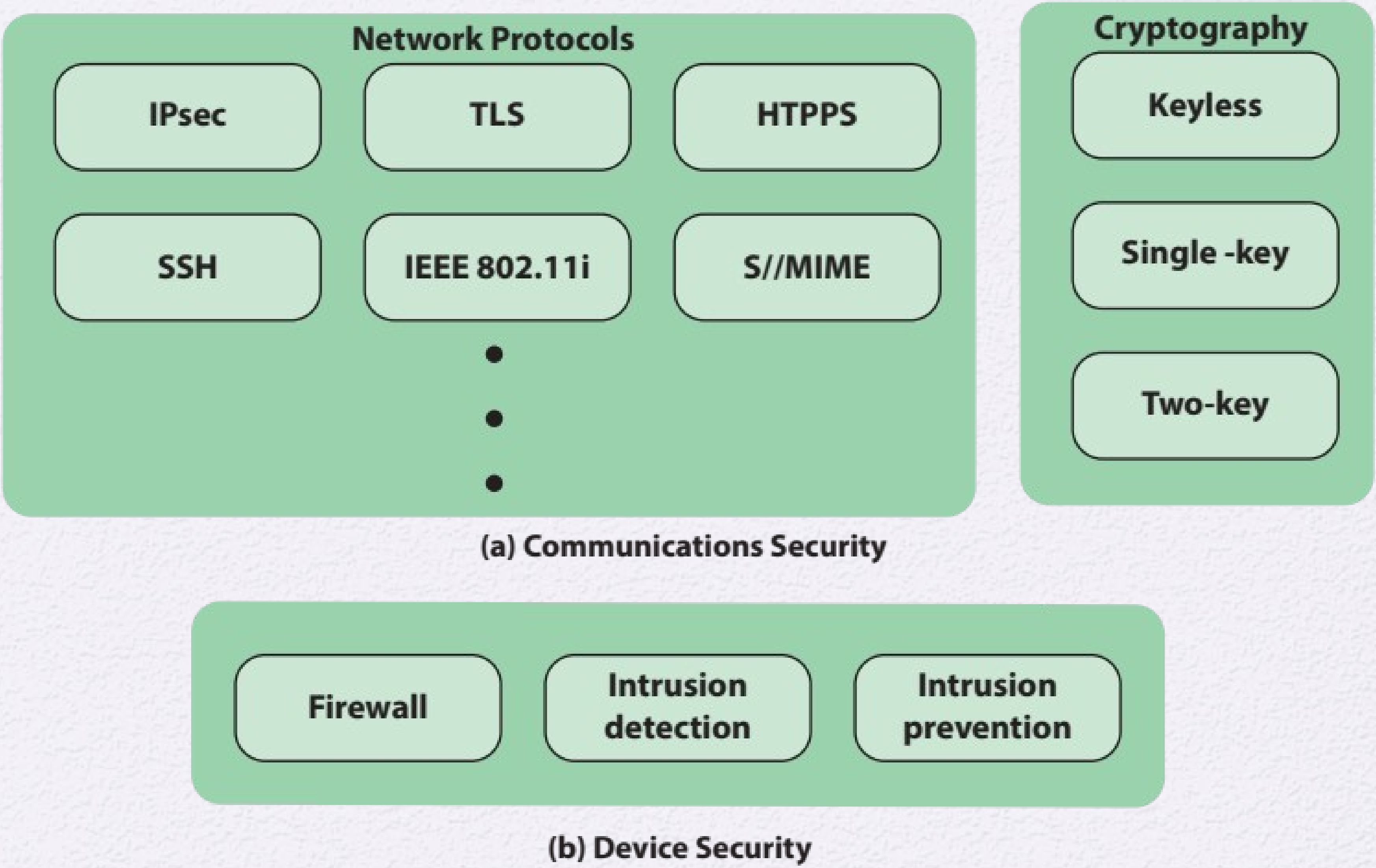


Figure 1.5 Key Elements of Network Security

Trust Model

- One of the most widely accepted and most cited definitions of trust is:

  “the willingness of a party (the trustor) to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”

- Three related concepts are relevant to a trust model:
  - **Trustworthiness**
  - **Propensity to trust**
  - **Risk:** typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence

- **Ability**: relates to the potential ability of the evaluated entity to do a given task or be entrusted with given information.
- **Benevolence**: trustworthy party has a genuine intention of goodwill towards the trusting party
- **Integrity**: It means that the trusting party (the truster) believes the other party (the trustee) follows a set of principles that the trusting party finds acceptable.

- The goal of model is, what course of action should trusting party take based on level of trust, and perceived risk.
  - Rely on trusted party to perform some actions.
  - The disclosure of information to the trusted party with the expectation that the information will be protected.

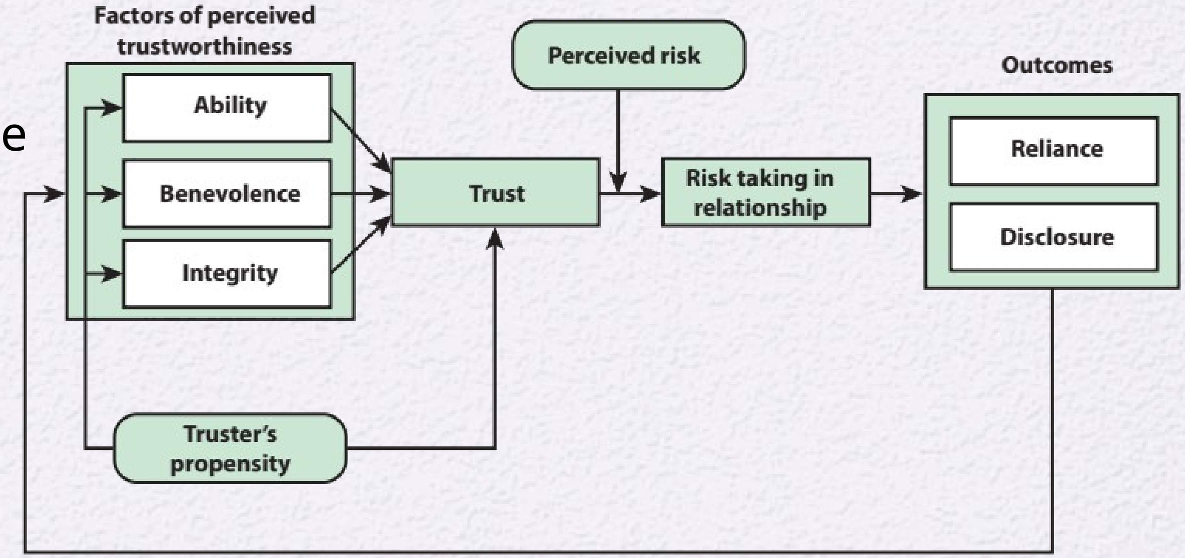


Figure 1.6 Trust Model

Mayer, R., Davis, J., and Schoorman, D. An Integrative Model of Organizational Trust. Academy of Management Review, July 1995.

Trust Model

The Trust Model and Information Security: an entity is said to trust a second entity when the first entity assumes that the second entity will behave exactly as the first entity expects. Entity might be hardware component, software module.

- Trustworthiness of an Individual
  - Internal users
  - External users
- Trustworthiness of an Organization
- Trustworthiness of an Information systems
  - Security functionality: security features (cryptographic algorithms)
  - Security assurance: audits.

Trust Model

Trustworthiness of an Individual

- **Internal users**
    - **Human resource security:** Sound security practice dictates that information security requirements be embedded into each stage of the employment life cycle
    - **Security awareness and training:** disseminating security information to
- **External users:** perceived trustworthiness and the truster's propensity, as discussed in last slide determine the level of trust.

Trust Model

Trustworthiness of an Organization

- Most organizations rely on information system service and information provided by external organizations, as well as partnerships to accomplish missions and business functions
  - Example: cloud service providers

- To manage risk to the organization, it must establish trust relationships with these external organizations
  - Such trust relationships can be: documenting the trust-related information in contracts, service-level agreements, statements of work.

Trust Model

Trustworthiness of an Information systems

- The degree to which information systems (including the information technology products from which the systems are built) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the systems across the full range of threats.

- Two factors affecting the trustworthiness of information systems are:
  - **Security functionality**: The security features/functions employed within the system.
  - **Security assurance**: Confidence in the effectiveness of security features and it is established with security management techniques like regular audits.

Establishing Trust Relationships

Validated trust:

- Trust is based on evidence obtained by the trusting organization about the trusted organization.
- For instance if organization develops application they can show that app meets requirements of certain security standard (evidence).

Direct historical trust:

- This type of trust is based on the security-related track record exhibited by an organization in the past, particularly in interactions with the organization seeking to establish trust

Mediated trust:

- A trust relationship that is established or maintained through an intermediary or a trusted third party rather than directly between two entities.

Mandated trust:

- Mandated trust means one organization trusts another because a higher authority tells them to.
- For instance, an organization might be authorized to issue digital certificates for a group of organizations. This authorization makes the other organizations trust them to handle this responsibility properly