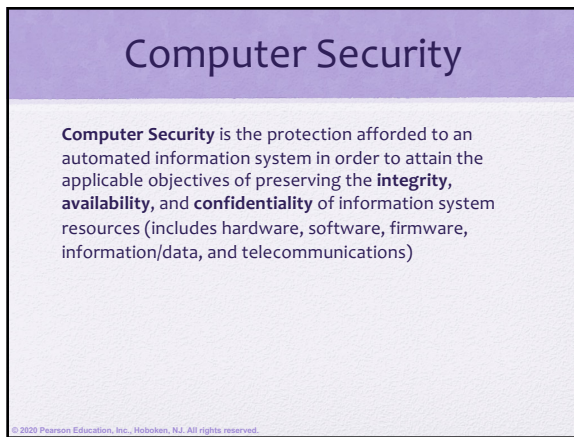
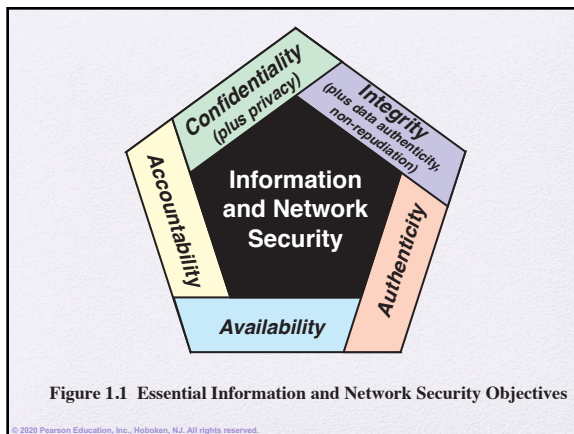


1



2



3

Security Objectives

- The cybersecurity definition introduces three key objectives that are at the heart of information and network 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

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

4

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
 - **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

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

5

Security Objectives

These three concepts form what is often referred to as the **CIA** triad. The three concepts embody the fundamental security objectives for both data and for information and computing services. In a nutshell:

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure
- **Integrity:** Guarding against improper information modification or destruction
- **Availability:** Ensuring timely and reliable access to and use of information

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

6

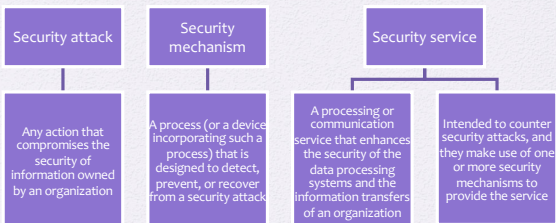
Security Objectives

- **Authenticity:** The property of being genuine and being able to be verified and Trusted. 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

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

7

OSI Security Architecture



© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

8

Threats and Attacks



Threat

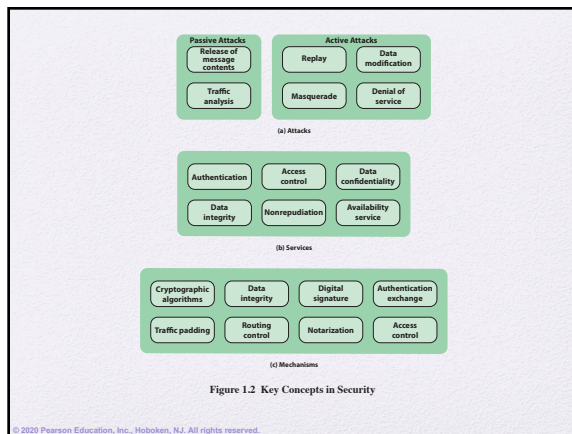
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

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.

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

9



10

Security Attacks


- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A *passive attack* attempts to learn or make use of information from the system but **does not affect system resources**
- An *active attack* attempts to **alter system resources or affect their operation**

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

11

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

12

Active Attacks

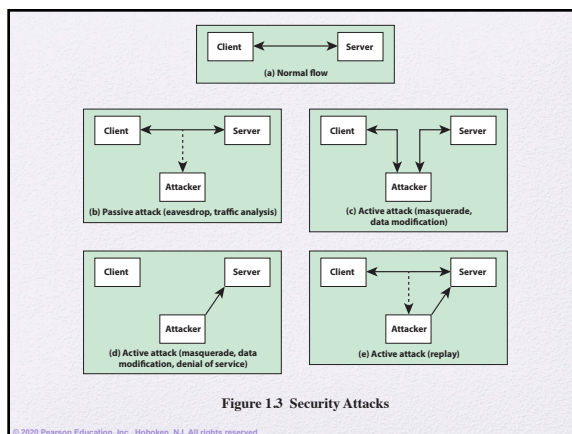
- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent** because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them



Masquerade	<ul style="list-style-type: none"> Takes place when one entity pretends to be a different entity Usually includes one of the other forms of active attack
Replay	<ul style="list-style-type: none"> Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
Data Modification	<ul style="list-style-type: none"> Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect
Denial of service	<ul style="list-style-type: none"> Prevents or inhibits the normal use or management of communications facilities

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

13



14

Authentication

- Concerned with assuring that a communication is authentic
 - 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

Two specific authentication services are defined in X.800:


- Peer entity authentication
- Data origin authentication

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

15

Access Control

- 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 identified, or authenticated, so that access rights can be tailored to the individual



© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

16

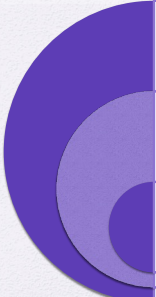
Data Confidentiality

- The protection of transmitted data from passive attacks
 - Broadest service protects all user data transmitted between two users over a period of time
 - Narrower forms of service includes the protection of a single message or even specific fields within a message
- The 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

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

17

Data Integrity



Can apply to a stream of messages, a single message, or selected fields within a message

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

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

18

Nonrepudiation

- 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



© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

19

Availability Service

- 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

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

20

Security Mechanisms

- **Cryptographic algorithms:** We can distinguish between reversible cryptographic mechanisms and irreversible cryptographic mechanisms. 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.
- **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.
- **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.

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

21

Service – Mechanism

Table 1.4 Relationship Between Security Services and Mechanisms

SERVICE	MECHANISM							
	Encipherment	Digital signature	Access control	Data integrity	Authentication	Authentication	Routing control	Non-repudiation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y	Y					
Nonrepudiation		Y	Y					Y
Availability			Y	Y				

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

22

Cryptographic algorithms can be grouped into three categories:

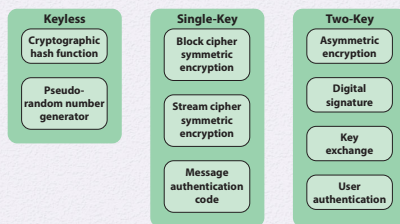


Figure 1.4 Cryptographic Algorithms

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

23

Summary

- Computer security concepts
- The OSI security architecture
- Provide an overview of the main areas of network security
- Security attacks
- Security services
- Security mechanisms
- Provide an overview of keyless, single-key and two-key cryptographic algorithms



© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

24
