Chapter 1

Computer and Network Security Concepts

Outline

- What is Cryptography?
- Computer security concepts
  - Definition
  - Examples
  - Challenges
- Security attacks
  - Passive attacks
  - Active attacks
- Security services
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
  - Availability service
- Security mechanisms

We will introduce/review quickly basic security concepts to illustrate the importance of Cryptography. This is NOT a security class!!!

Cryptography Definition

- Historical (dictionary) definition:
  - The art of **writing** or **solving codes**

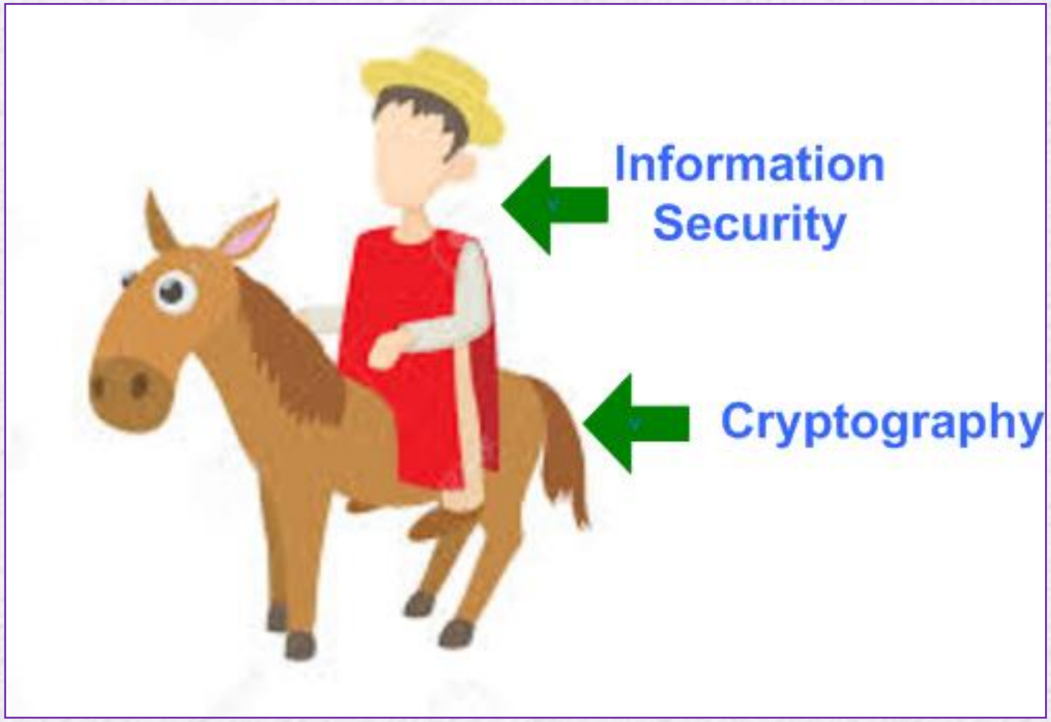
- Modern cryptography
  - Scientific **study** of **techniques** for **securing**:
    - digital **information**,
    - **transactions**, and
    - distributed **computations.**

  (Katz, Lindell)

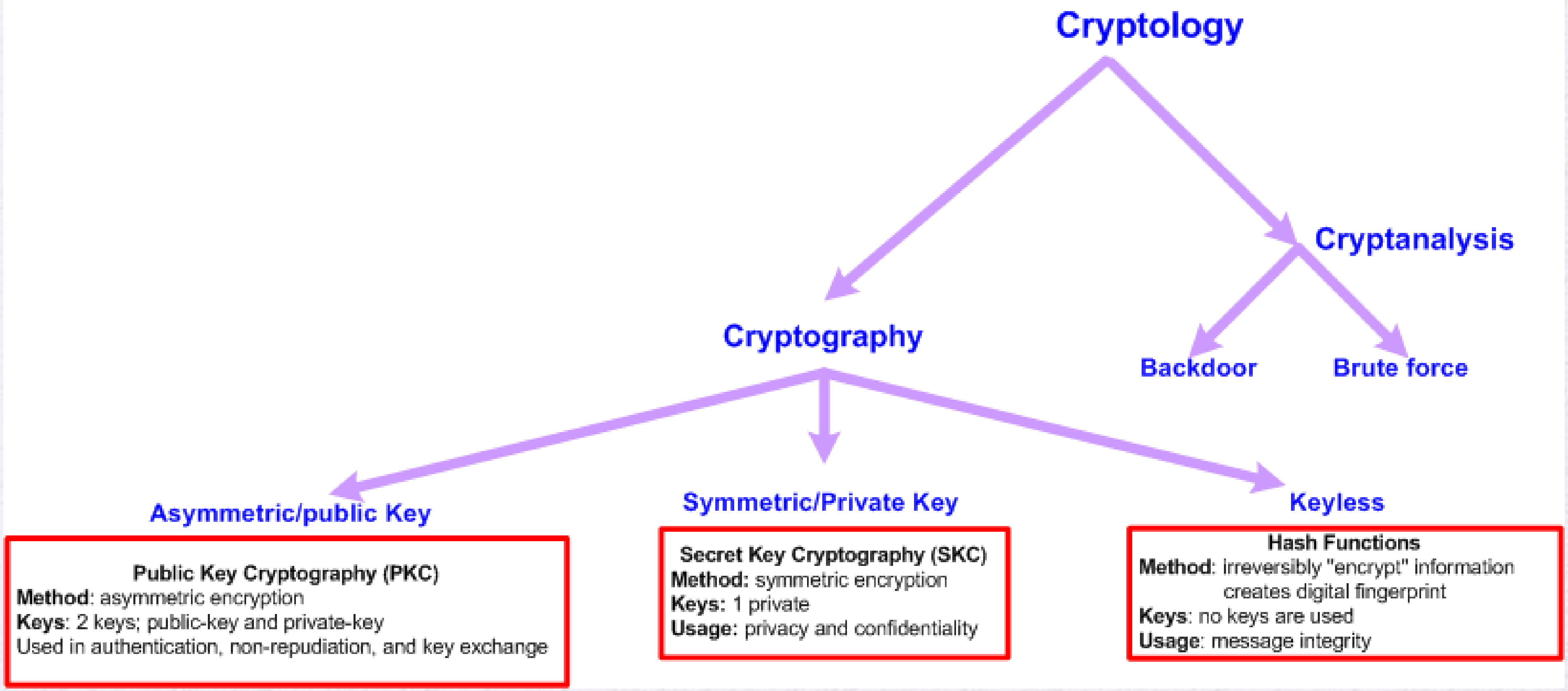
- **Cryptanalysis** is the science (and sometimes art) of breaking cryptosystems.

Cryptography and Security

- Cryptography provides techniques (services) for information security.



Cryptography



Cryptology

Cryptography

Cryptanalysis

Backdoor

Brute force

Asymmetric/public Key

Public Key Cryptography (PKC)
Method: asymmetric encryption
Keys: 2 keys; public-key and private-key
Used in authentication, non-repudiation, and key exchange

Symmetric/Private Key

Secret Key Cryptography (SKC)
Method: symmetric encryption
Keys: 1 private
Usage: privacy and confidentiality

Keyless

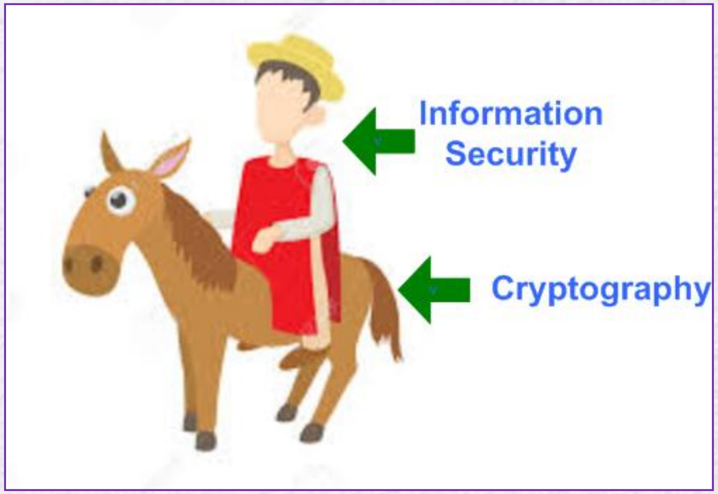
Hash Functions
Method: irreversibly "encrypt" information creates digital fingerprint
Keys: no keys are used
Usage: message integrity

Cryptography Techniques

	Asymmetric	Symmetric	Hash
Keys	Public and private keys	Private Key	No Key
Provides	Confidentiality, Integrity, Authentication, Non-repudiation	Confidentiality, Integrity, Authentication, Non-repudiation	Integrity, Origin Authentication
Advantages	Key management: secure + easy	Small key size	No Key
Disadvantage	Key length is large, requires complex computation	Key management; n(n-1)/2 keys; manual distribution	Less Secure

Review Of Important Security Concepts

- The goal of the next few slides is to demonstrate the relation between cryptography and security.
- For more in-depth security concepts and analysis: refer to the security course.



Cryptographic algorithms and protocols can be grouped into four main areas:

Symmetric encryption

- Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords

Asymmetric encryption

- Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures

Data integrity algorithms

- Used to protect blocks of data, such as messages, from alteration

Authentication protocols

- Schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

The field of network and Internet security consists of:

measures to 1 deter, 2 prevent, 3 detect, and 4 correct **security violations** that involve the transmission of information

Computer Security

The NIST *Computer Security Handbook* defines the term computer security as:

> “the **protection** afforded to an automated **information system** in order to attain the applicable **objectives** of preserving the **integrity**, **availability** and **confidentiality** of information system resources” (includes hardware, software, firmware, information/ data, and telecommunications)

Computer Security Objectives

Confidentiality

- 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

- 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

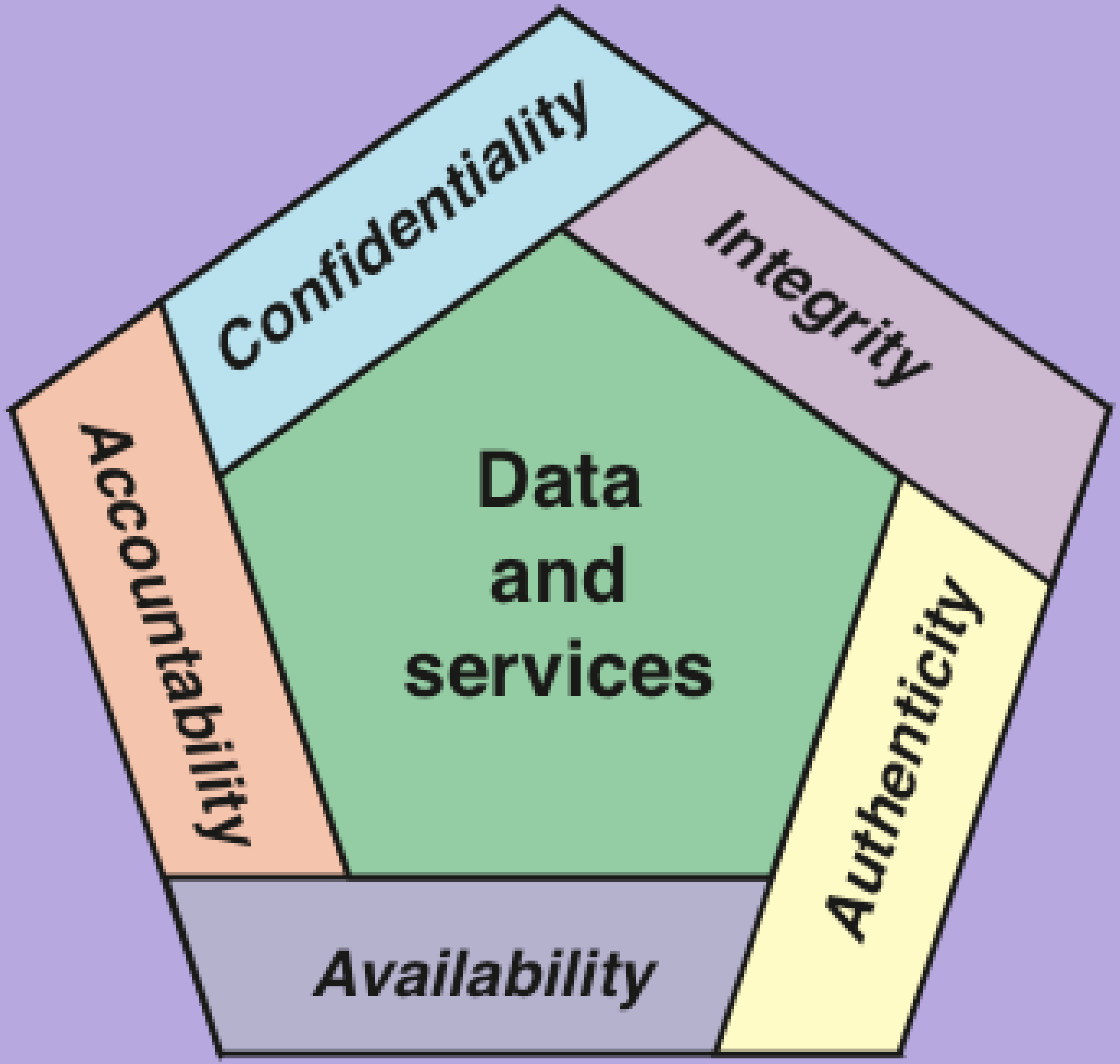
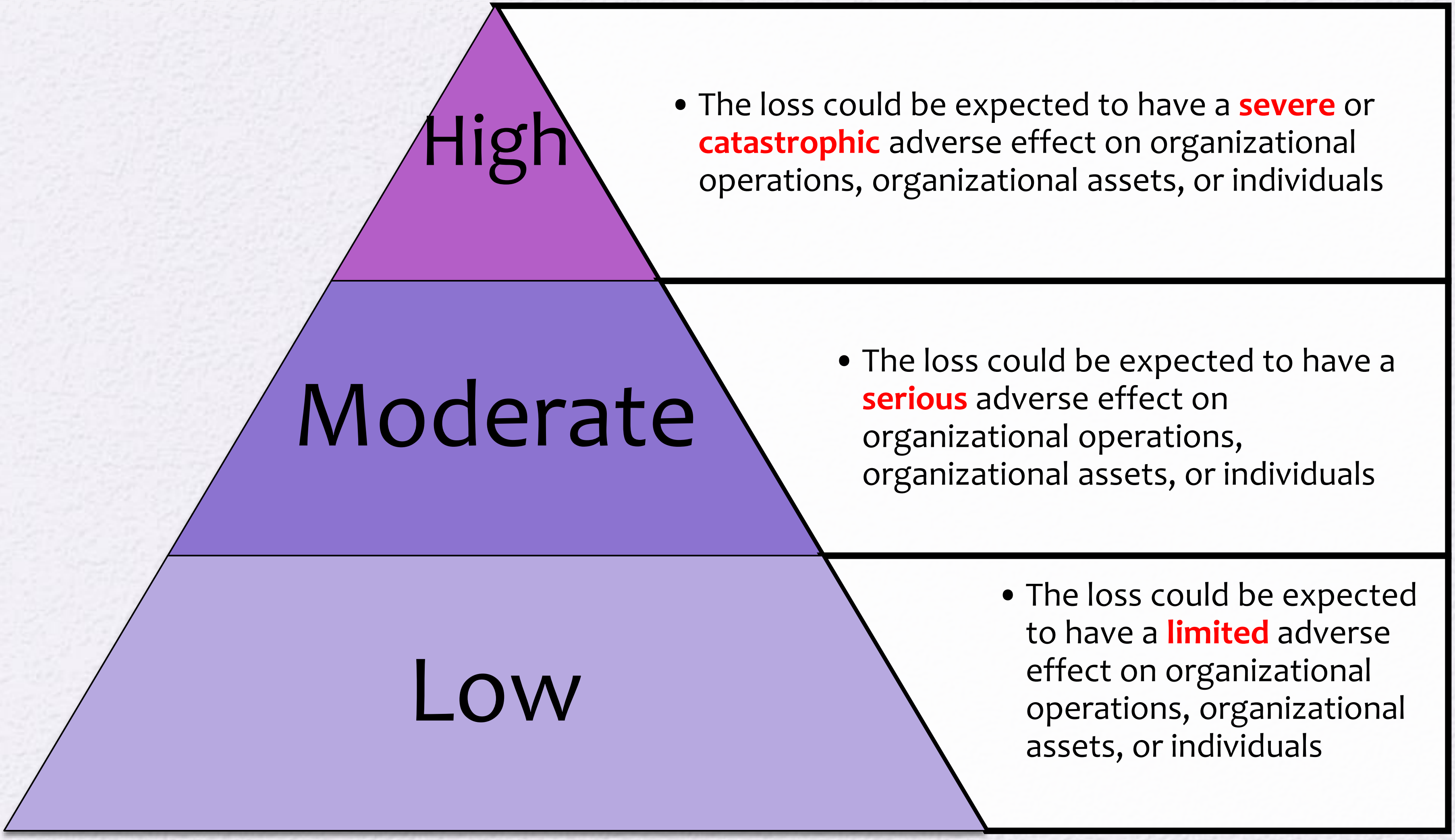


Figure 1.1 Essential Network and Computer Security Requirements

Breach of Security
Levels of Impact



High

- The loss could be expected to have a **severe** or **catastrophic** adverse effect on organizational operations, organizational assets, or individuals

Moderate

- The loss could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals

Low

- The loss could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals

Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- 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

OSI Security Architecture

- **The Open System Interconnect (OSI)**
- **Security attack**
  - Any **action** that **compromises the security** of information owned by an organization.
    - **Security threat** is a **potential** of security breach/violation.
- **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
  - Intended to **counter security attacks**, and they make **use of one or more security mechanisms** to provide the service

Security Attacks

- A *passive attack* attempts to learn or make use of information from the system but **neither alter system resources nor affect system operation**

- An *active attack* attempts to **alter system resources or affect their operation**

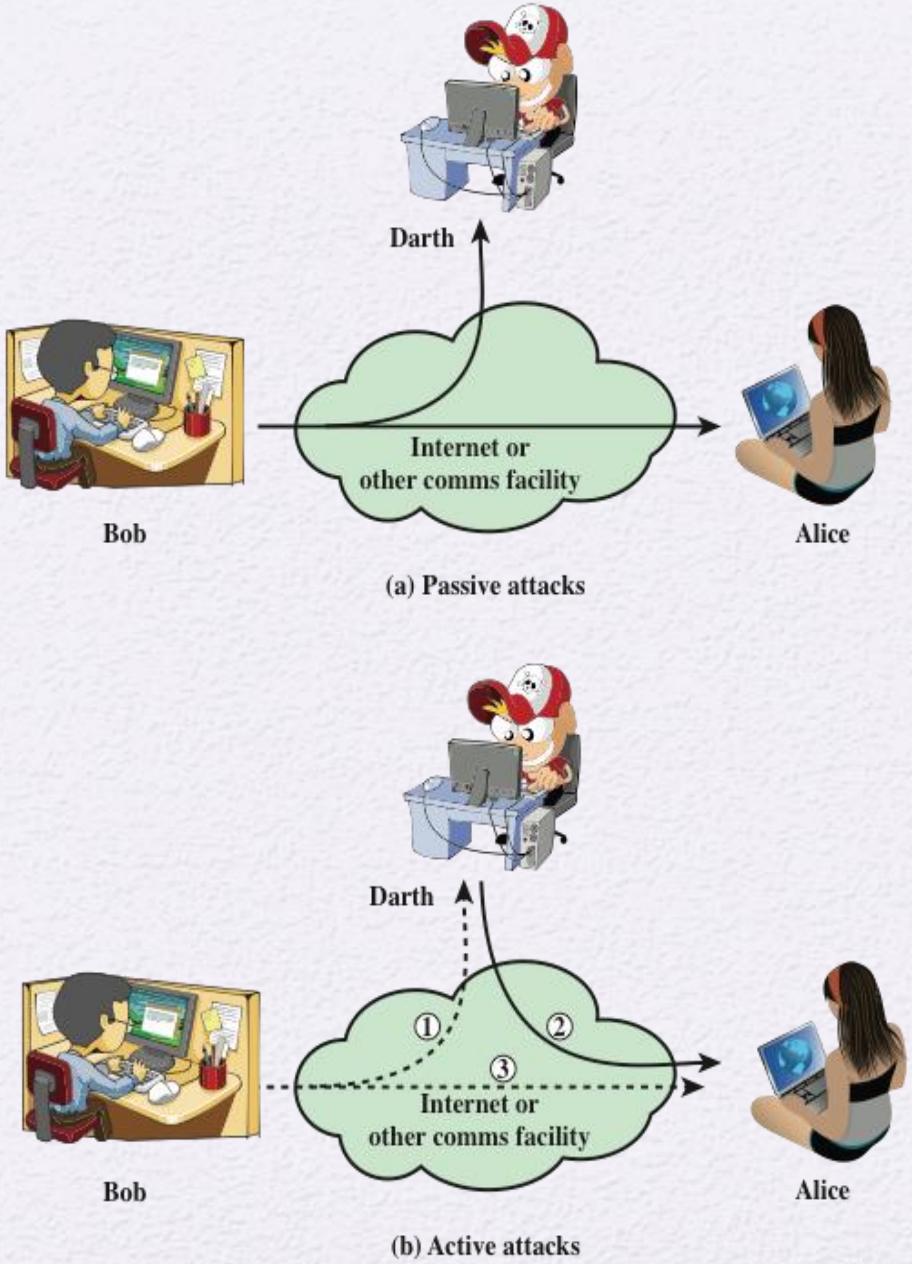


Figure 1.2 Security Attacks

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 Examples

- 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

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

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

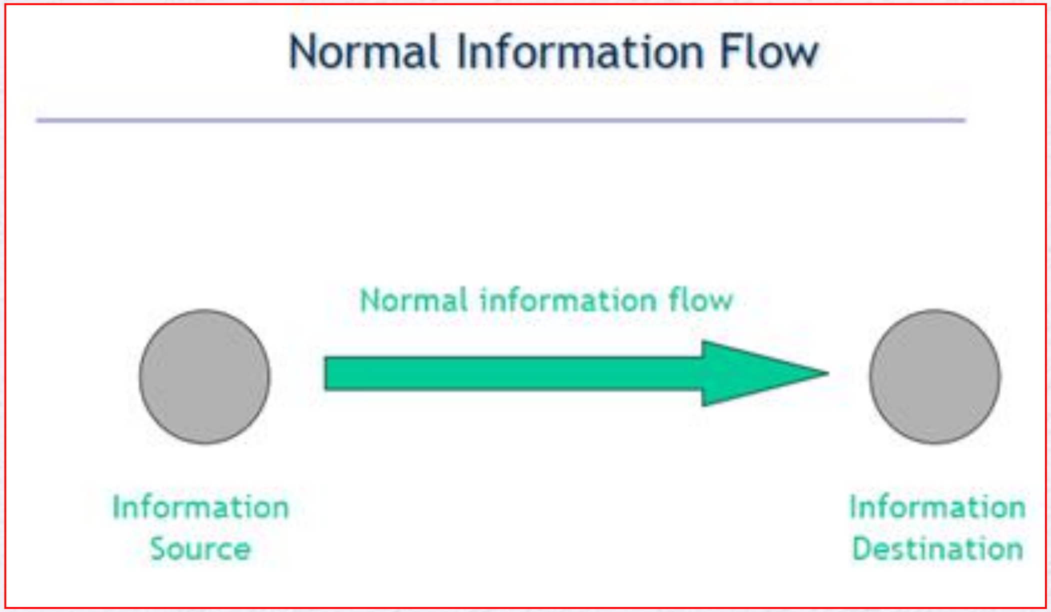
Modification of messages

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

Denial of service

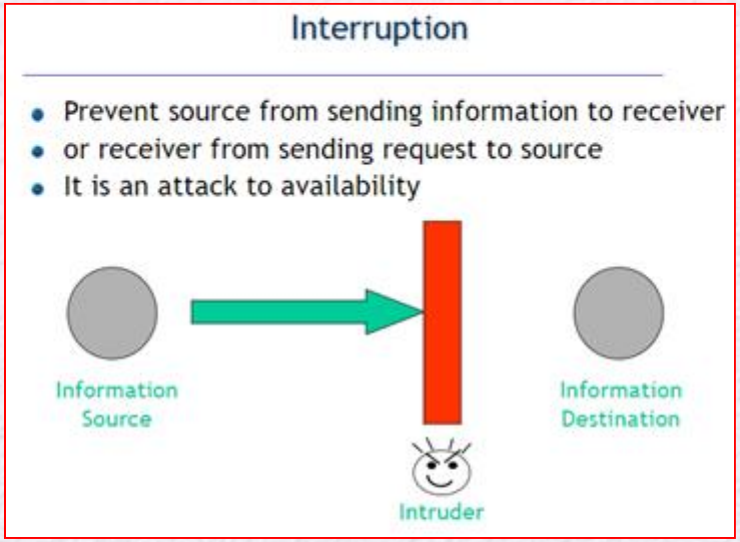
- Prevents or inhibits the normal use or management of communications facilities

Normal Information Flow and Attacks: Examples



Normal Information Flow

Attack on Availability

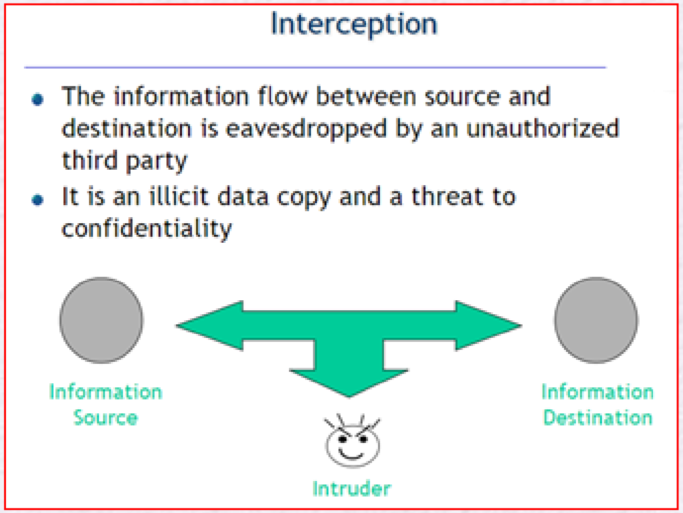


Interruption

- Prevent source from sending information to receiver
- or receiver from sending request to source
- It is an attack to availability

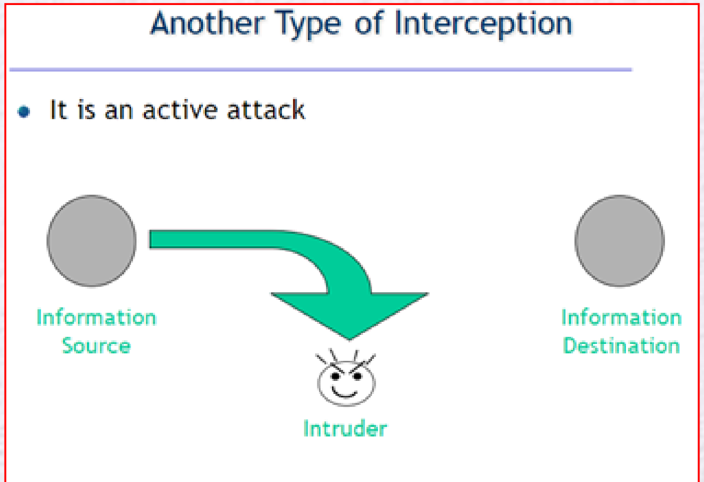
Attack on confidentiality and integrity: examples

Attack on confidentiality



Interception

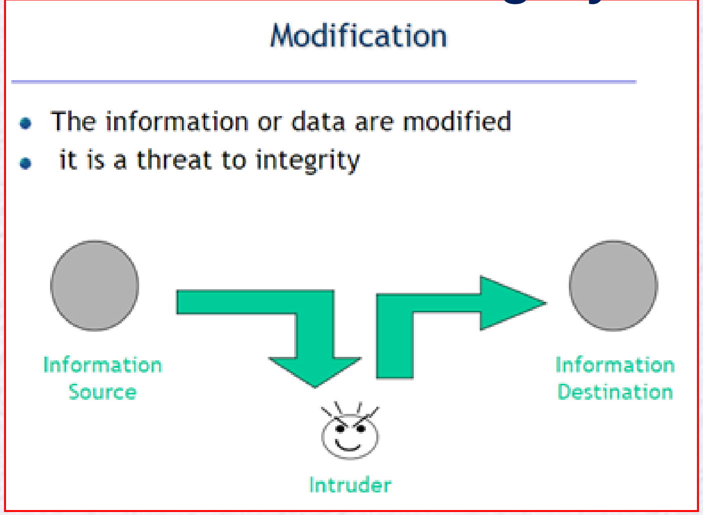
- The information flow between source and destination is eavesdropped by an unauthorized third party
- It is an illicit data copy and a threat to confidentiality



Another Type of Interception

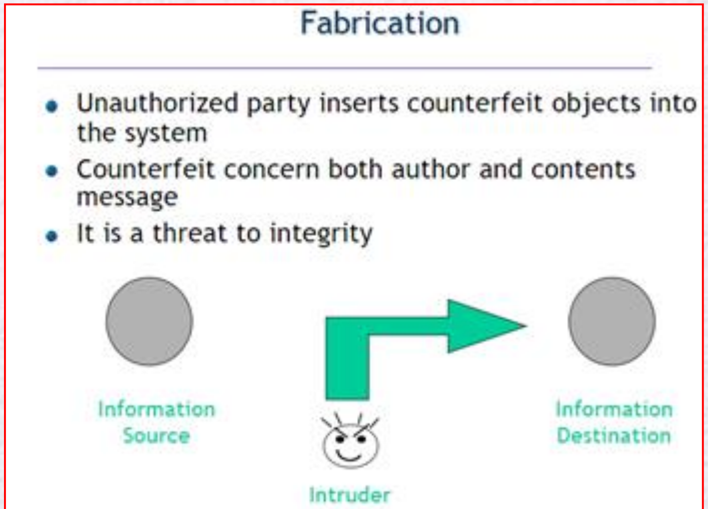
- It is an active attack

Attack on integrity



Modification

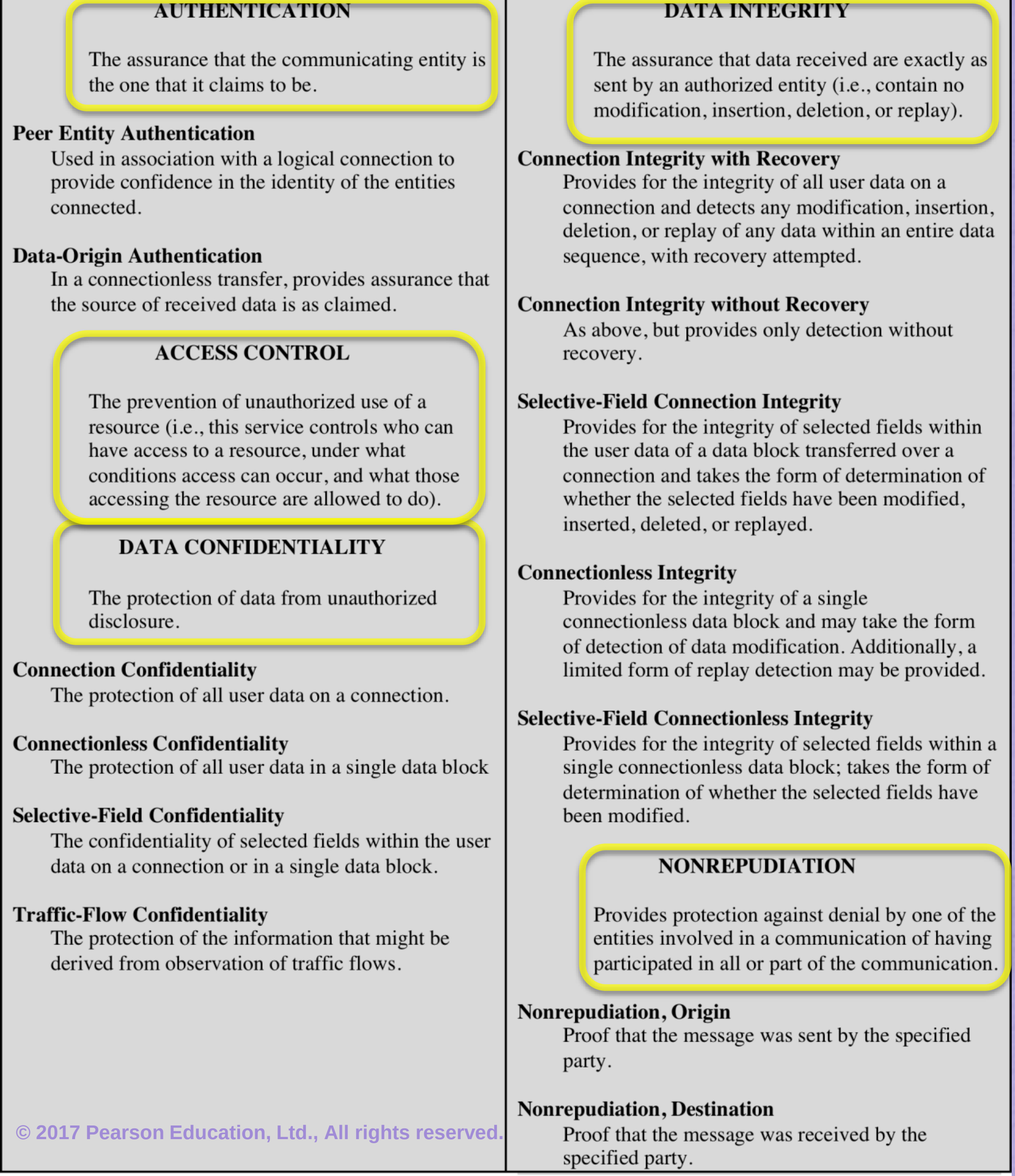
- The information or data are modified
- it is a threat to integrity



Fabrication

- Unauthorized party inserts counterfeit objects into the system
- Counterfeit concern both author and contents message
- It is a threat to integrity

Security Services (X.800)



AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

(This table is found on page 12 in textbook)

Authentication

- Concerned with assuring that a communication is authentic
  - **Data origin authentication**: In the case of a single message, **assures** the recipient that **the message is from intended source** that it claims to be from
  - **Peer entity authentication**: 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

Access Control

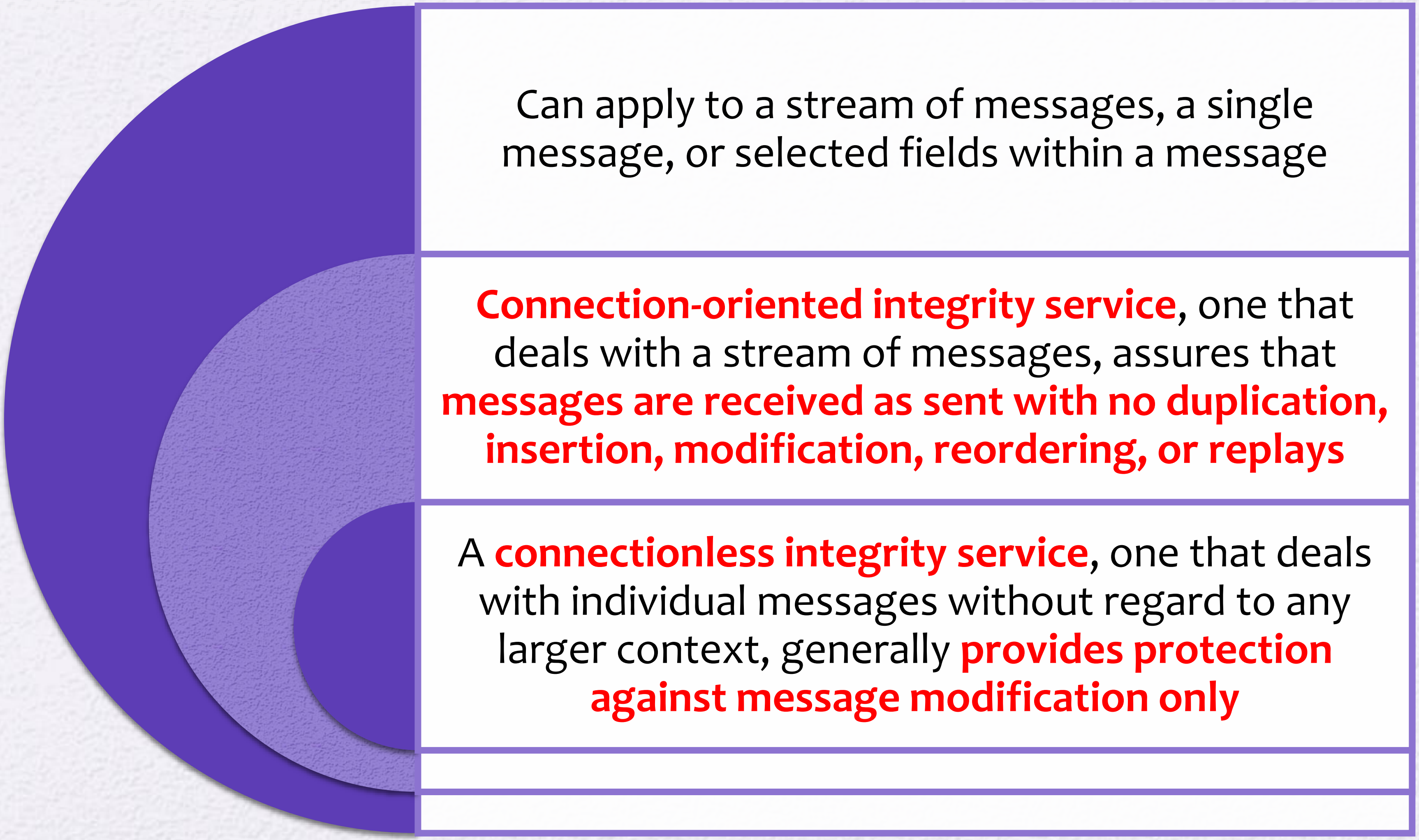
- The ability to limit and **control the access to host systems and applications** via communications links

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

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

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**

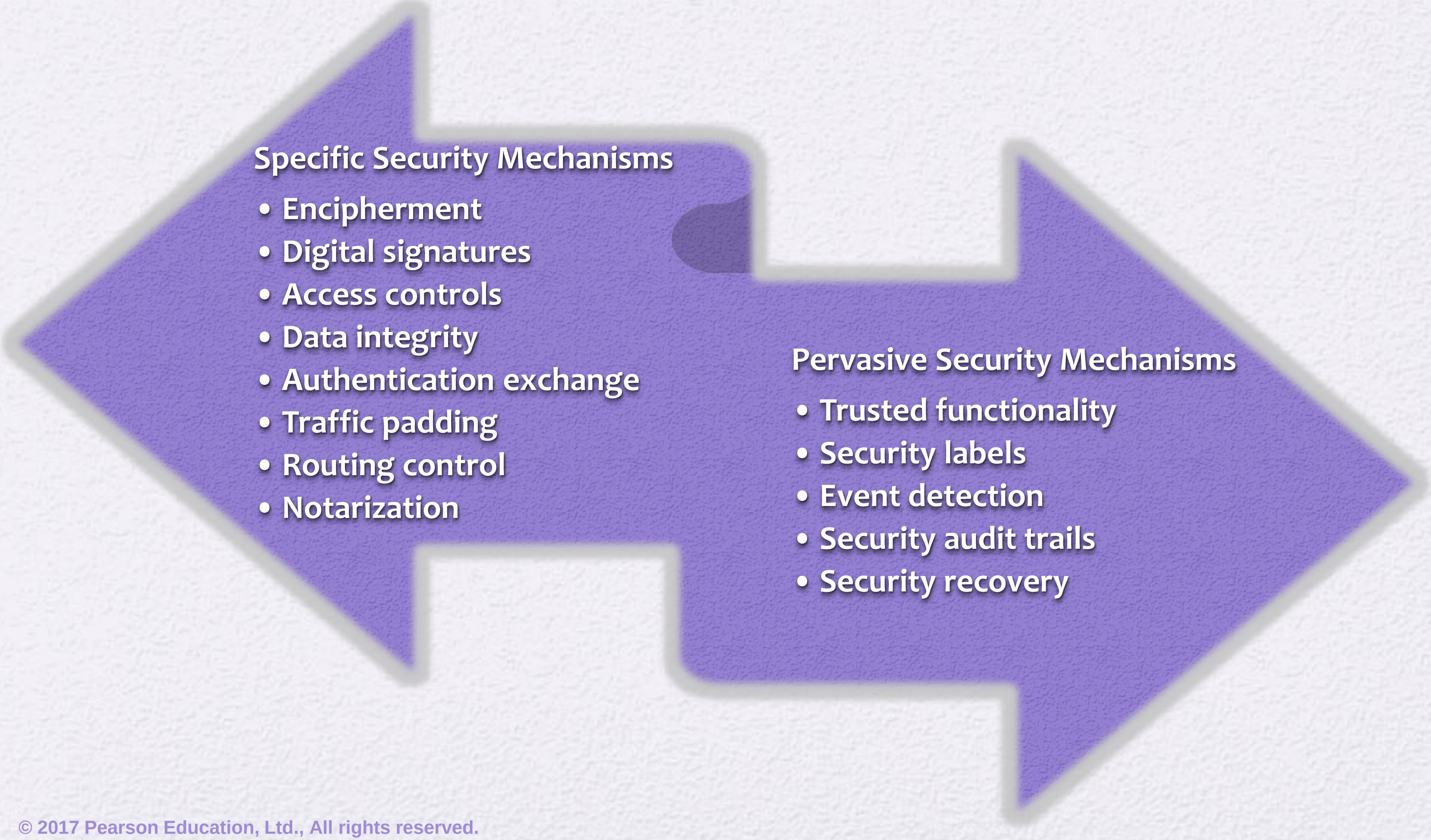
Nonrepudiation

- **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

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

Security Mechanisms

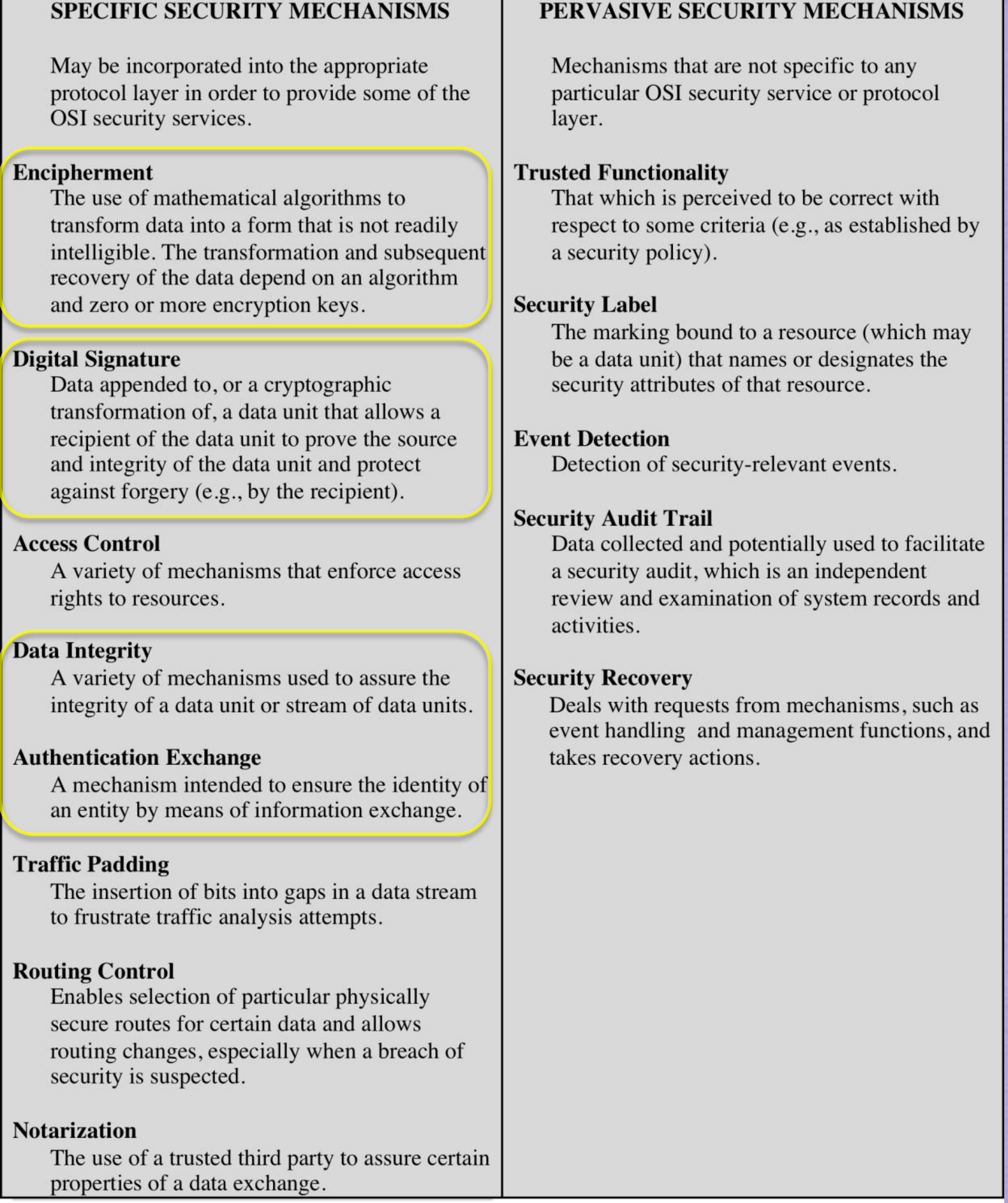


Specific Security Mechanisms

- Encipherment
- Digital signatures
- Access controls
- Data integrity
- Authentication exchange
- Traffic padding
- Routing control
- Notarization

Pervasive Security Mechanisms

- Trusted functionality
- Security labels
- Event detection
- Security audit trails
- Security recovery



SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment
The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

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 (e.g., by the recipient).

Access Control
A variety of mechanisms that enforce access rights to resources.

Data Integrity
A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

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 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.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality
That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection
Detection of security-relevant events.

Security Audit Trail
Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Security Recovery
Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Table 1.3

Security Mechanisms (X.800)

(This table is found on pages 14-15 in textbook)