Cryptography and Network Security
Overview & Chapter 1

Fifth Edition

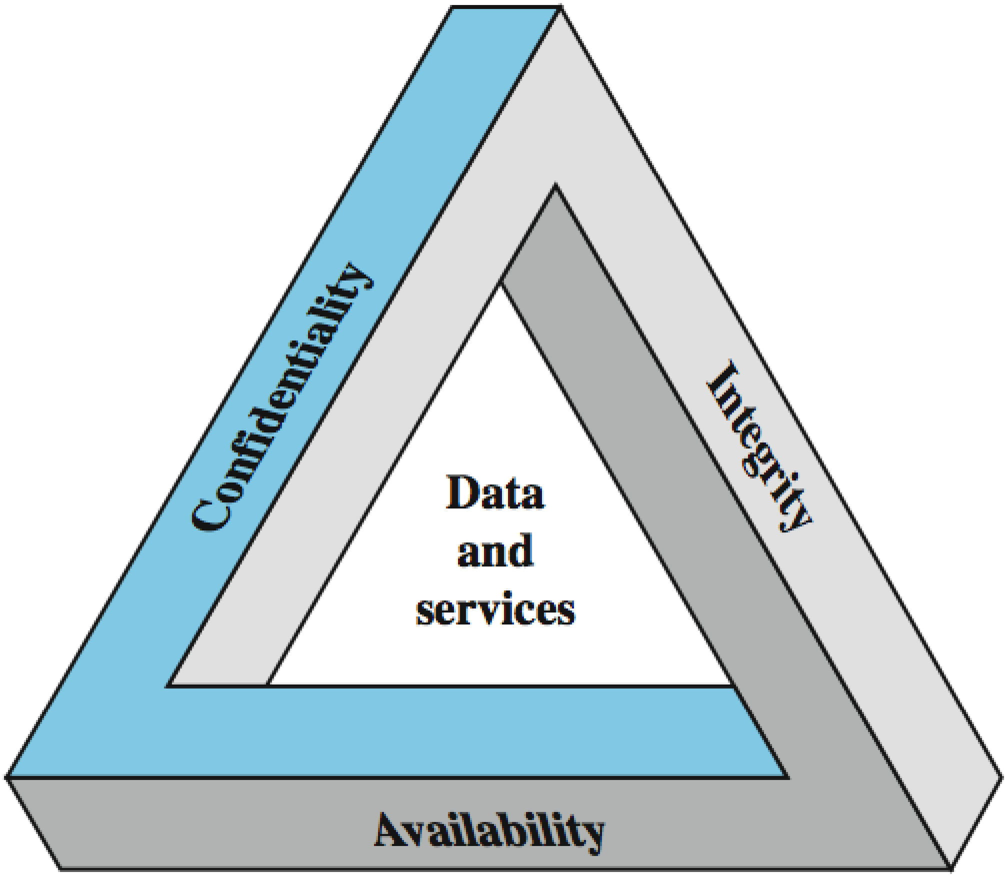
by William Stallings

Lecture slides by Lawrie Brown

Objectives

- ❑ To define three security goals
- ❑ To define security attacks that threaten security goals
- ❑ To define security services and how they are related to the three security goals
- ❑ To define security mechanisms to provide security services
- ❑ To introduce two techniques, cryptography and steganography, to implement security mechanisms.

Key Security Concepts



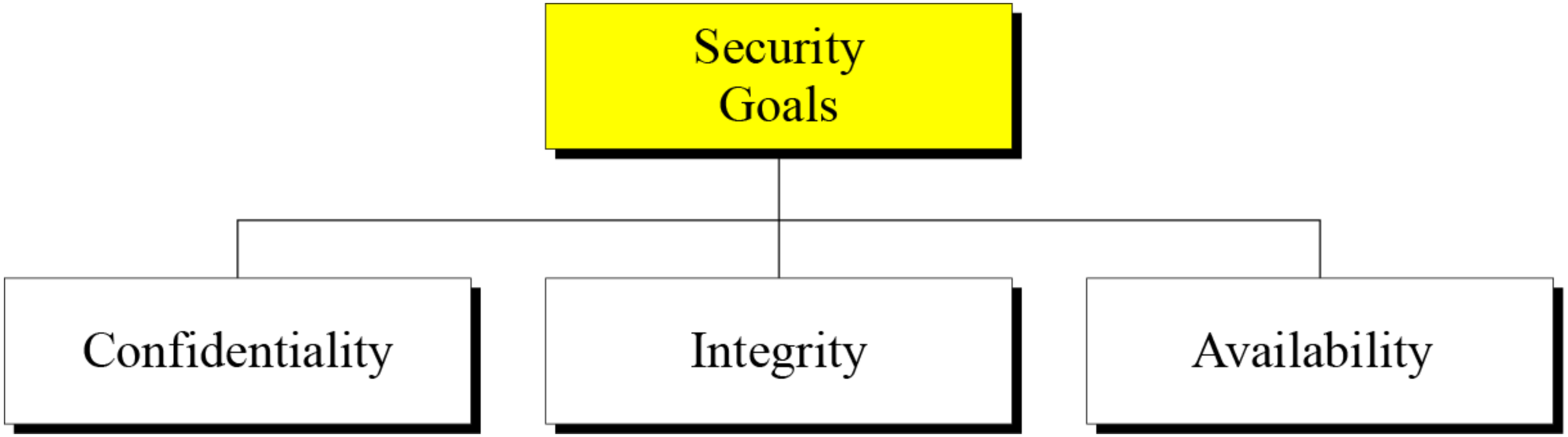
Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – The loss of the service translates into a large financial loss

Aspects of Security

- consider 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**
- note terms
  - *threat* – a potential for violation of security
  - *attack* – an assault on system security, a deliberate attempt to evade security services

Taxonomy of security goals



Security Goals

Confidentiality

Integrity

Availability

Confidentiality

Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

Integrity

Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

Availability

The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.

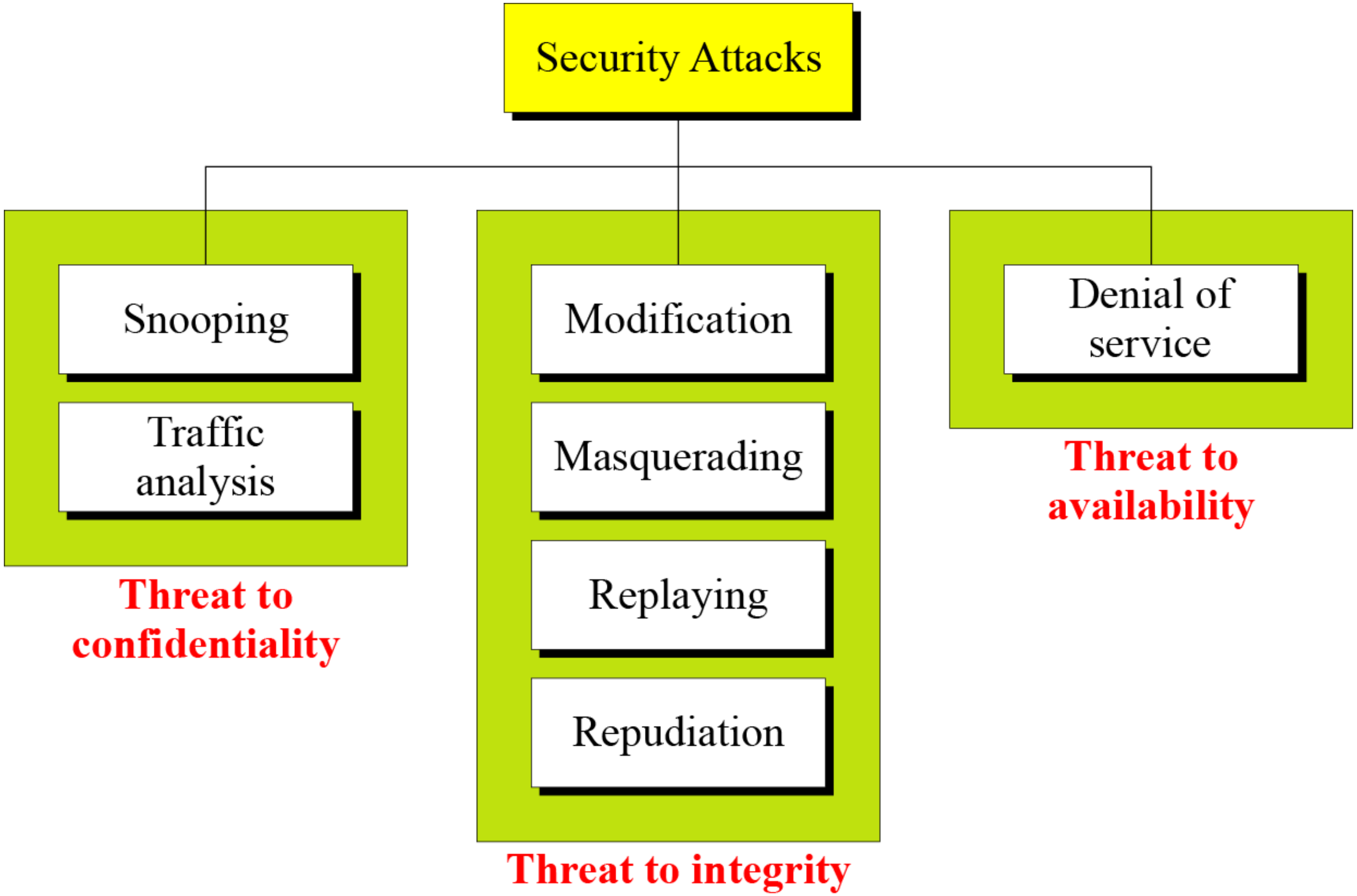
ATTACKS

The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.

Topics discussed in this section:

1.2.1 Attacks Threatening Confidentiality
1.2.2 Attacks Threatening Integrity
1.2.3 Attacks Threatening Availability
1.2.4 Passive versus Active Attacks

Taxonomy of attacks with relation to security goals



Security Attacks

Snooping

Traffic analysis

Threat to confidentiality

Modification

Masquerading

Replaying

Repudiation

Threat to integrity

Denial of service

Threat to availability

Attacks Threatening Confidentiality

Snooping refers to unauthorized access to or interception of data.

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

Attacks Threatening Integrity

Modification means that the attacker intercepts the message and changes it.

Masquerading or spoofing happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

Attacks Threatening Availability

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

A sever class of this attack is the Distributed Denial of service (DDoS) attack. In this class very large number (thousands or even millions) of attacking machines are coordinated and synchronized to attack a victim system simultaneously.

Passive Versus Active Attacks

Passive attacks

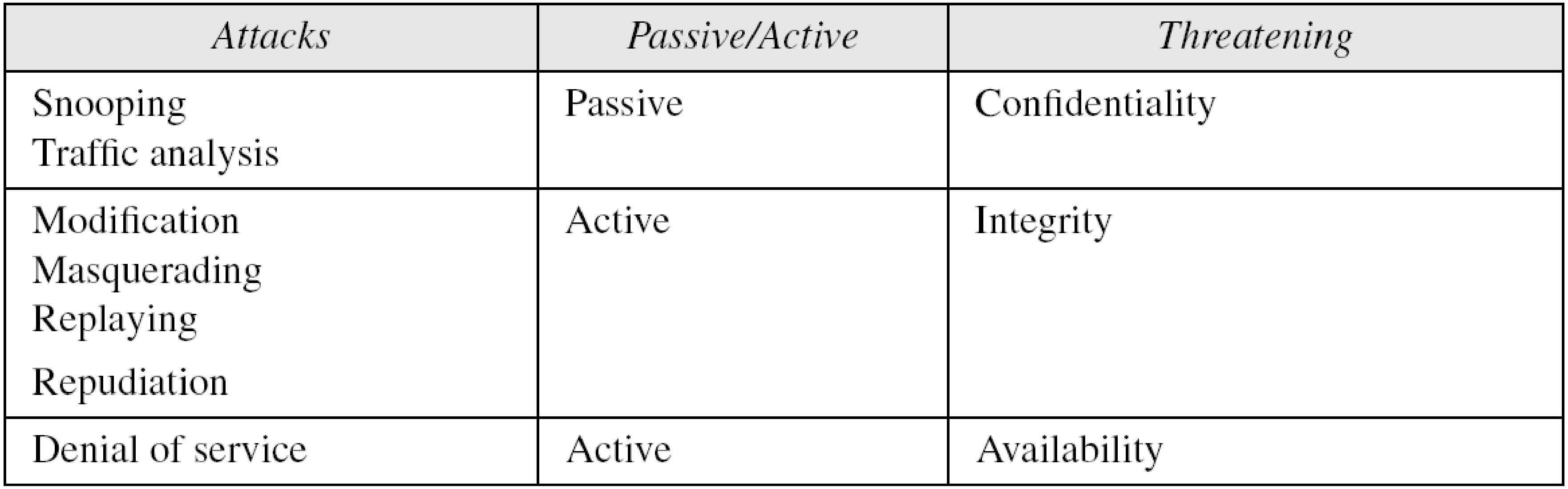
1. Release of message contents (Snooping - التطفل): unauthorized reading of a message.
2. Traffic analysis: useful in guessing the nature of the communication between two parties.

Active attacks

1. Masquerade: to impersonate the identity of someone.
2. Replay: to get an unauthorized copy of a message and resend it afterwards.
3. Modification of messages: to add, delete , or modify some contents of a message.
4. Repudiation: The sender of a message will deny sending; or the recipient will deny receiving.
5. Denial of Service (DoS): to prevent authorized users from accessing resources such as data or servers or networks.

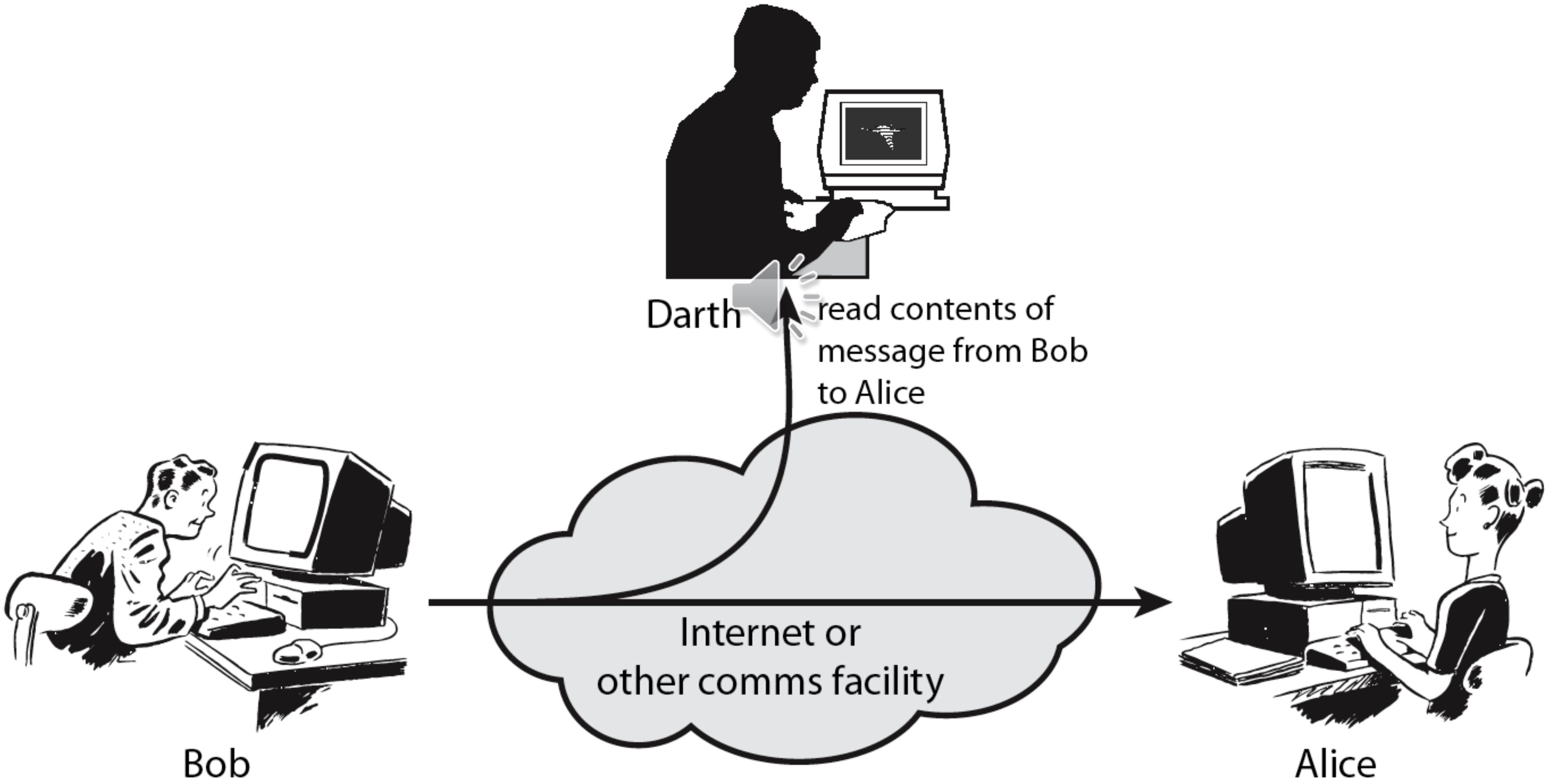
Passive Versus Active Attacks

Summary



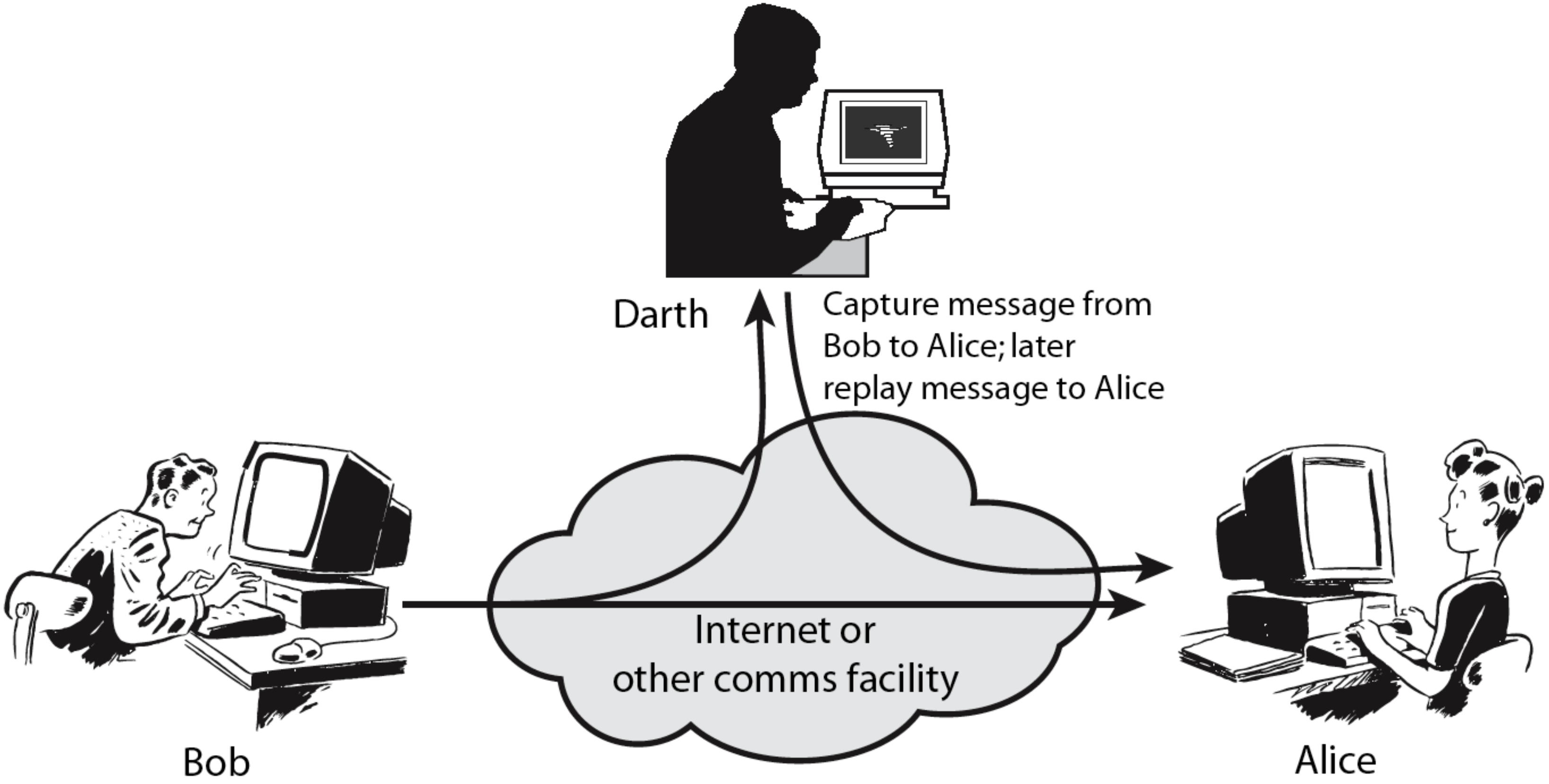
Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Passive Attacks


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Release of message contents (Snooping)

Active Attacks


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Replay attack

SERVICES AND MECHANISMS

As standardized by the International Telecommunication Union;
Telecommunication Standardization Sector (ITU-T)

ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.

Topics discussed in this section:

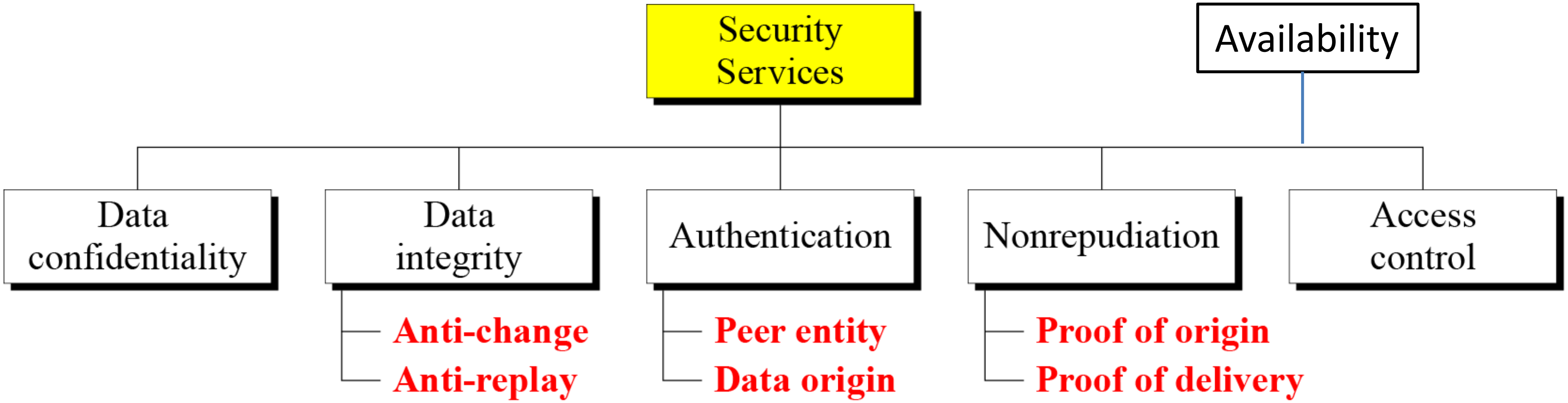
1.3.1 Security Services
1.3.2 Security Mechanism
1.3.3 Relation between Services and Mechanisms

Security Services

(As recommended in the X.800 Protocol of the ITU-T)

- **Authentication** - assurance that communicating entity is the one claimed
  - peer-entity authentication
  - data origin authentication
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication
- **Availability** – resource accessible and usable

Security Services



The security service is defined in the Internet document RFC 2828 as follows:

“A processing or communication service provided by a system to give a specific kind of protection to system resources”

Security Mechanisms in the X.800 Protocol

Specific Security Mechanisms

- Encryption,
- Digital signatures,
- Access controls,
- Data integrity,
- Authentication exchange,
- Traffic padding,
- Routing control,
- Notarization. (التوثيق)

X.800 Definitions of the Mechanisms

Encryption

The cryptographic transformation of data to produce ciphertext.

Digital signatures

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 controls

Access control mechanisms may be applied at either end of a communications association and/or at any intermediate point. Access controls involved at the origin or any intermediate point are used to determine whether the sender is authorized to communicate with the recipient and/or to use the required communications resources.

Data integrity

Two aspects of data integrity are: the integrity of a single data unit or field; and the integrity of a stream of data units or fields.

X.800 Definitions of the Mechanisms

Authentication exchange

A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic padding

The generation of spurious instances of communication, spurious data units and/or spurious data within data units.

Routing control

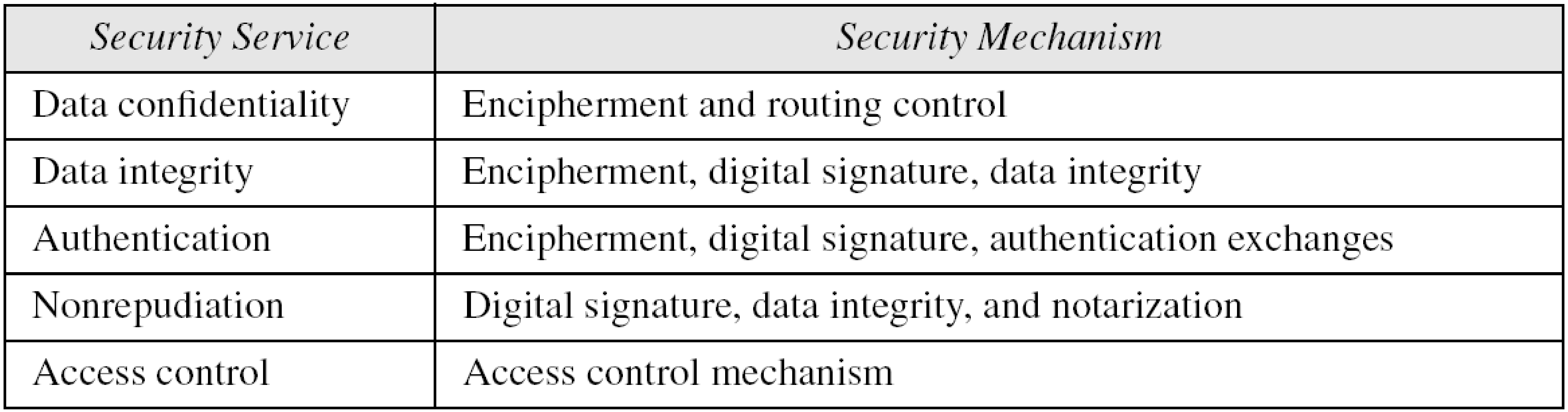
The application of rules during the process of routing to chose or avoid specific networks, links or relays.

Notarization

The **registration of data with a trusted third party** that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery.

Relation between Services and Mechanisms

Table 1.2 Relation between security services and mechanisms



Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

***Encipherment:** this another name for encryption.*

Characteristics of a Security Service

1. Enhance security of data processing systems and information transfers of an organization
2. Intended to counter security attacks
3. Using one or more security mechanisms
4. Often replicates functions normally associated with physical documents which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

1-4 TECHNIQUES

Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today:

1. Cryptography
2. Steganography

Cryptography

Cryptography, a word with Greek origins, means “secret writing.” However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

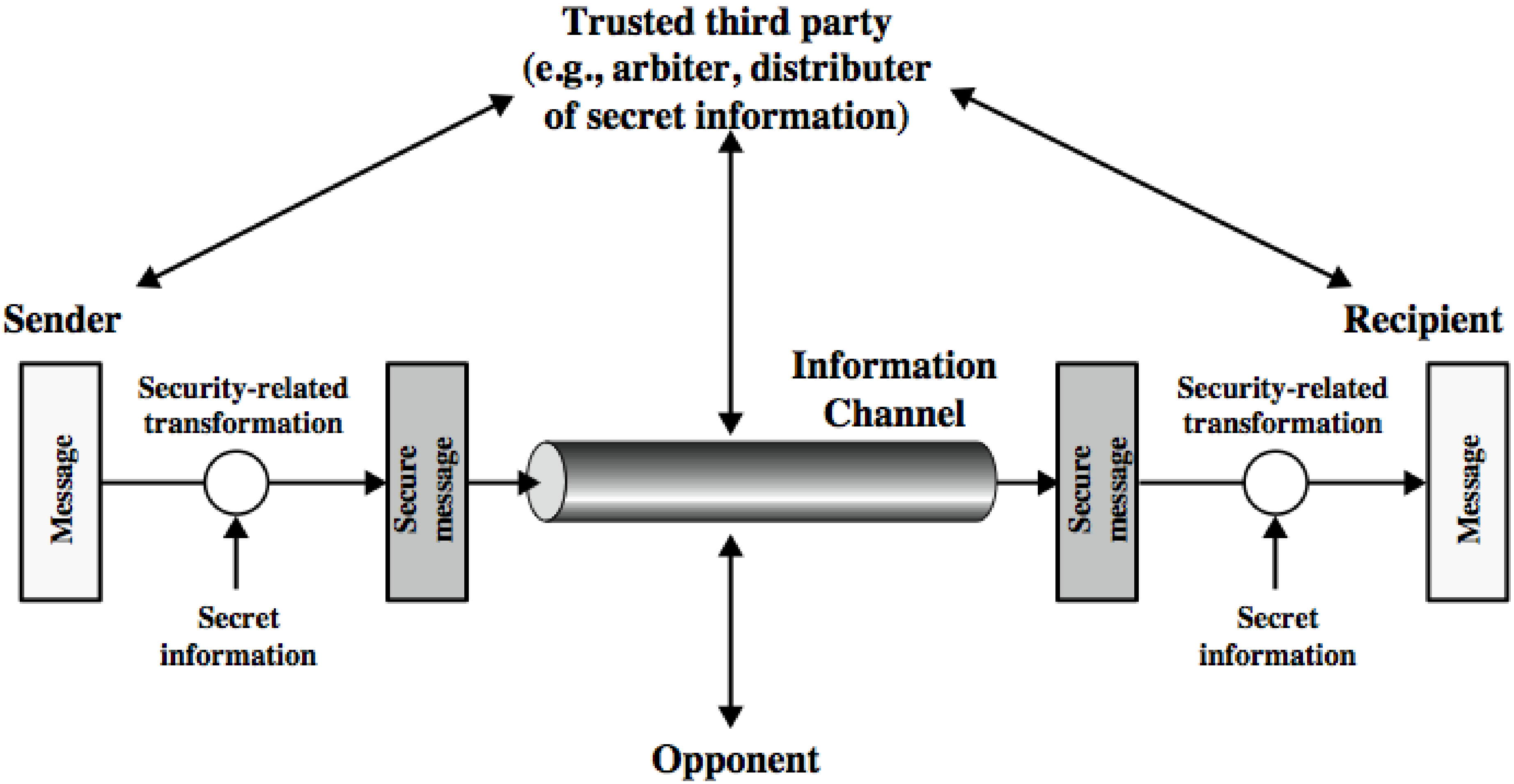
Steganography

The word steganography, with origin in Greek, means "covered writing," in contrast with cryptography, which means "secret writing."

Example

1. Convert your data into a stream of "N" bits, say N=10000 bits.
2. Use an image, audio or video file to carry the data bits. The carrying file must have a number of bytes much more than "N".
3. To carry the data bits, select "N" bytes of the carrying file and replace the least significant bit in each selected byte by a single data bit. There will be minor distortion in the carrying file that would not be noticed.
4. Send the carrying file to its recipient.
5. At the receiving side, the data bits can be extracted in a reverse order.

Model for Network Security

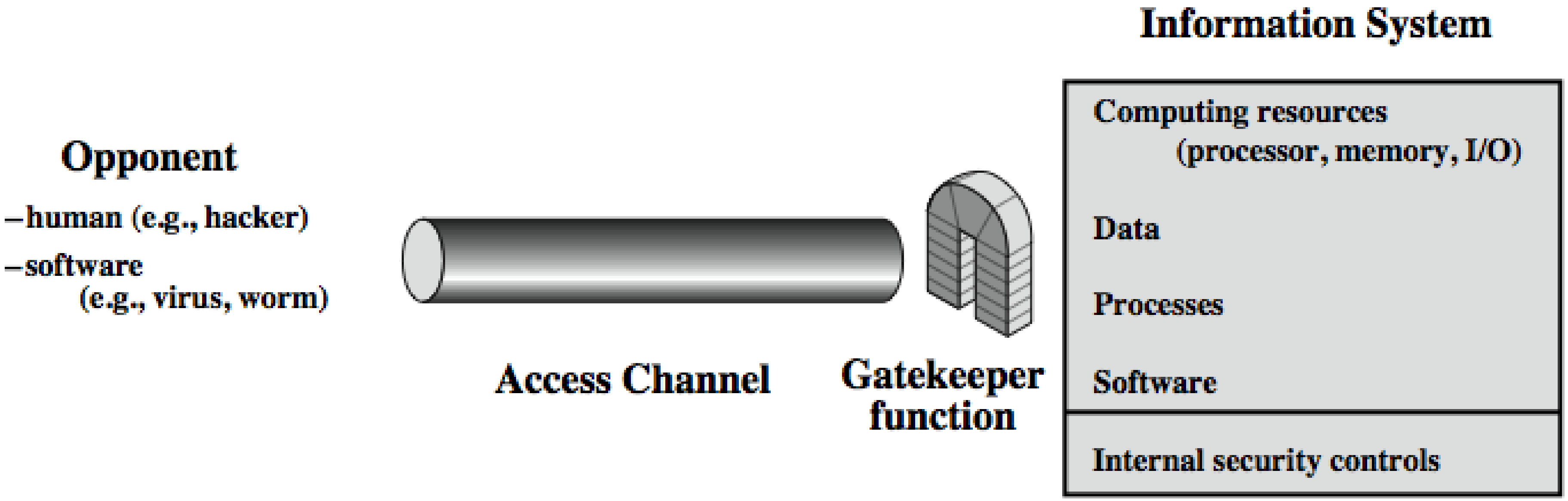


Topics Related to the Network Security Model

Using this model requires us to:

1. Design a suitable algorithm for the security transformation
2. Generate the secret information (keys) used by the algorithm
3. Develop methods to distribute and share the secret information
4. Specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



- The gatekeeper is typically a firewall.
- The internal security controls ensure that only authorized users can access designated information or resources, for example *username* and *password*, or biometric authentication such as sound identification.

Summary

Topics covered in this chapter are:

1. Security concepts: confidentiality, integrity, and availability.
2. X.800 security architecture.
3. Security attacks, services, mechanisms.
4. Models for network (access) security.