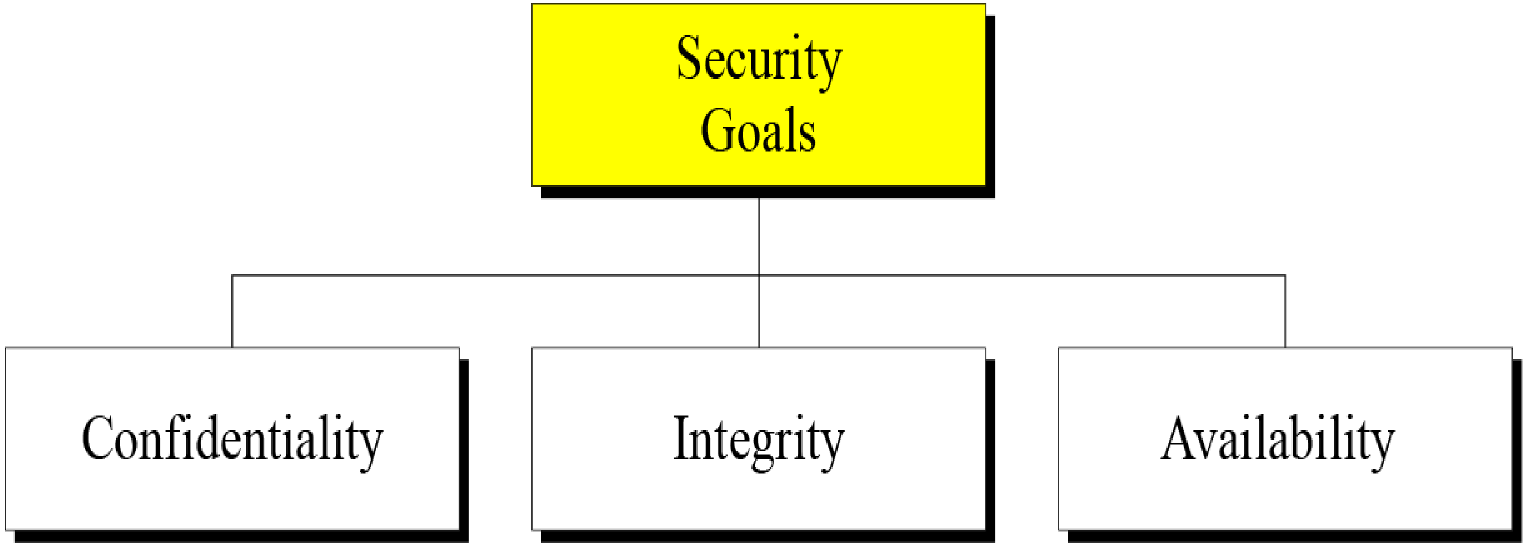
Definition of Information Security

The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

Security Goals



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.

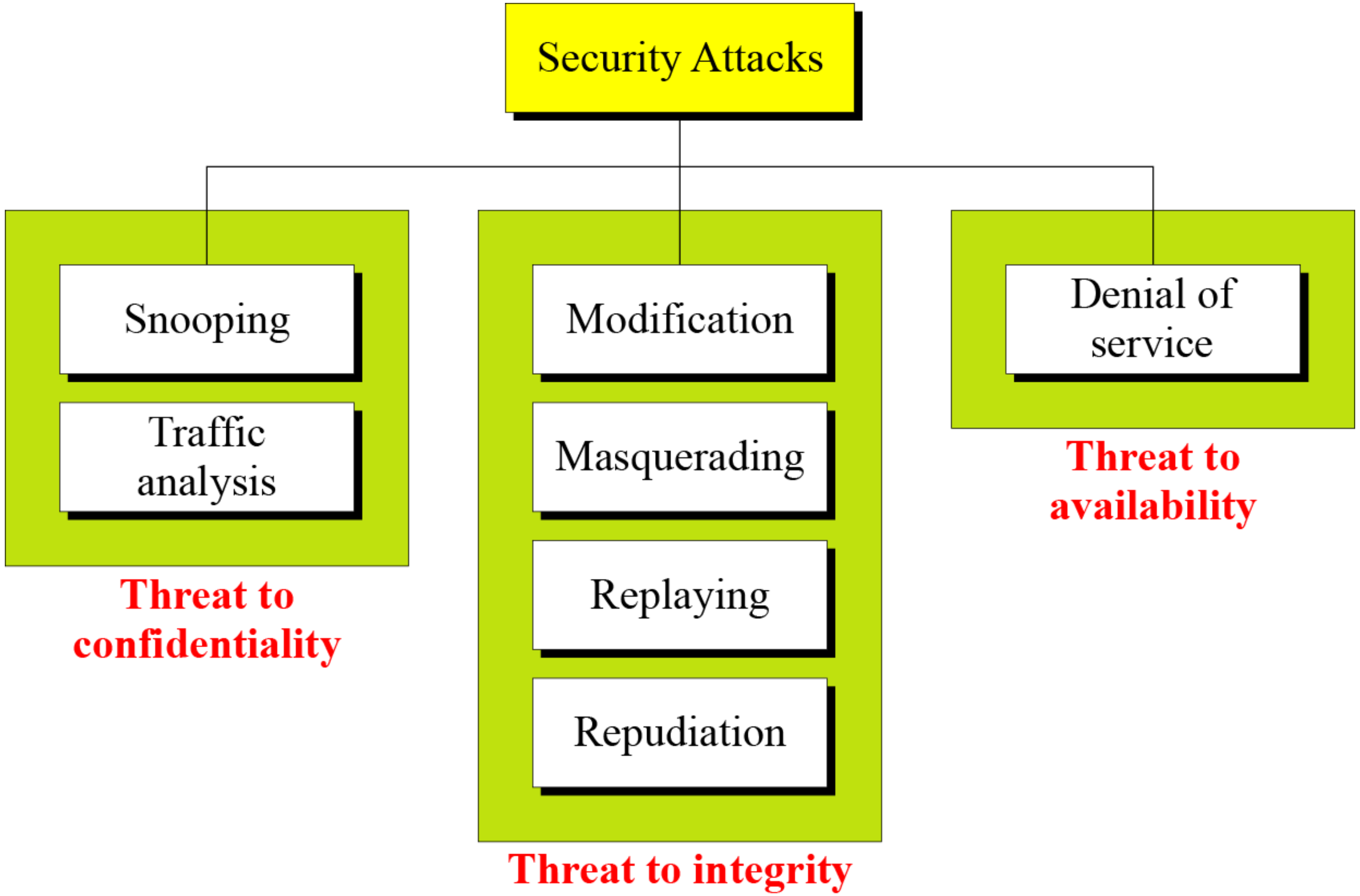
ATTACKS

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

Attacks Threatening Confidentiality
Attacks Threatening Integrity
Attacks Threatening Availability
Passive versus Active Attacks

ATTACKS Contd.

Taxonomy of attacks with relation to security goals



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.

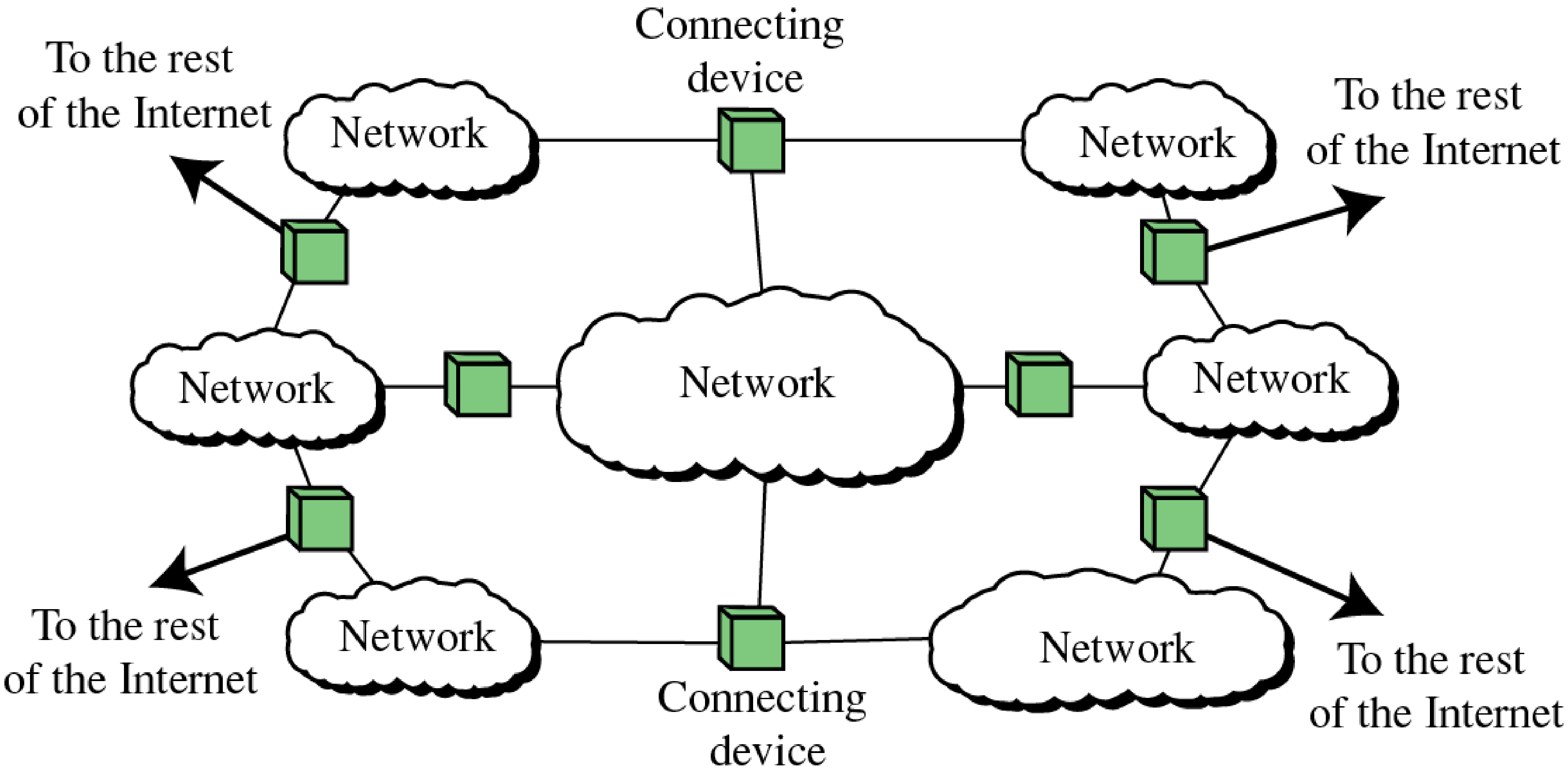
Attacks Threatening Integrity

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.

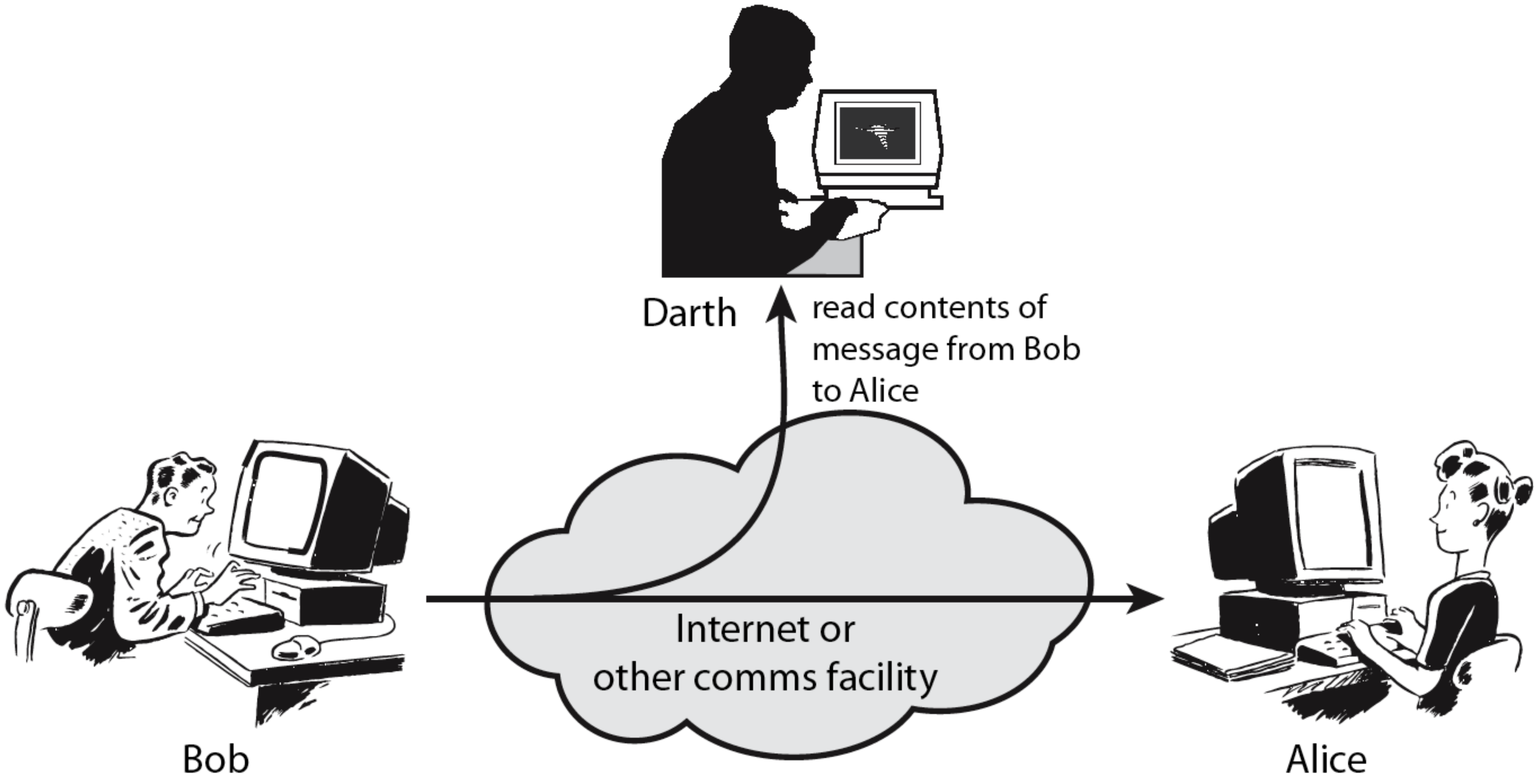
Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.


Connecting
device
To the rest
of the Internet
Network
Network
To the rest
of the Internet
Network
Network
Network
Network
To the rest
of the Internet
Network
Network
To the rest
of the Internet
Connecting
device

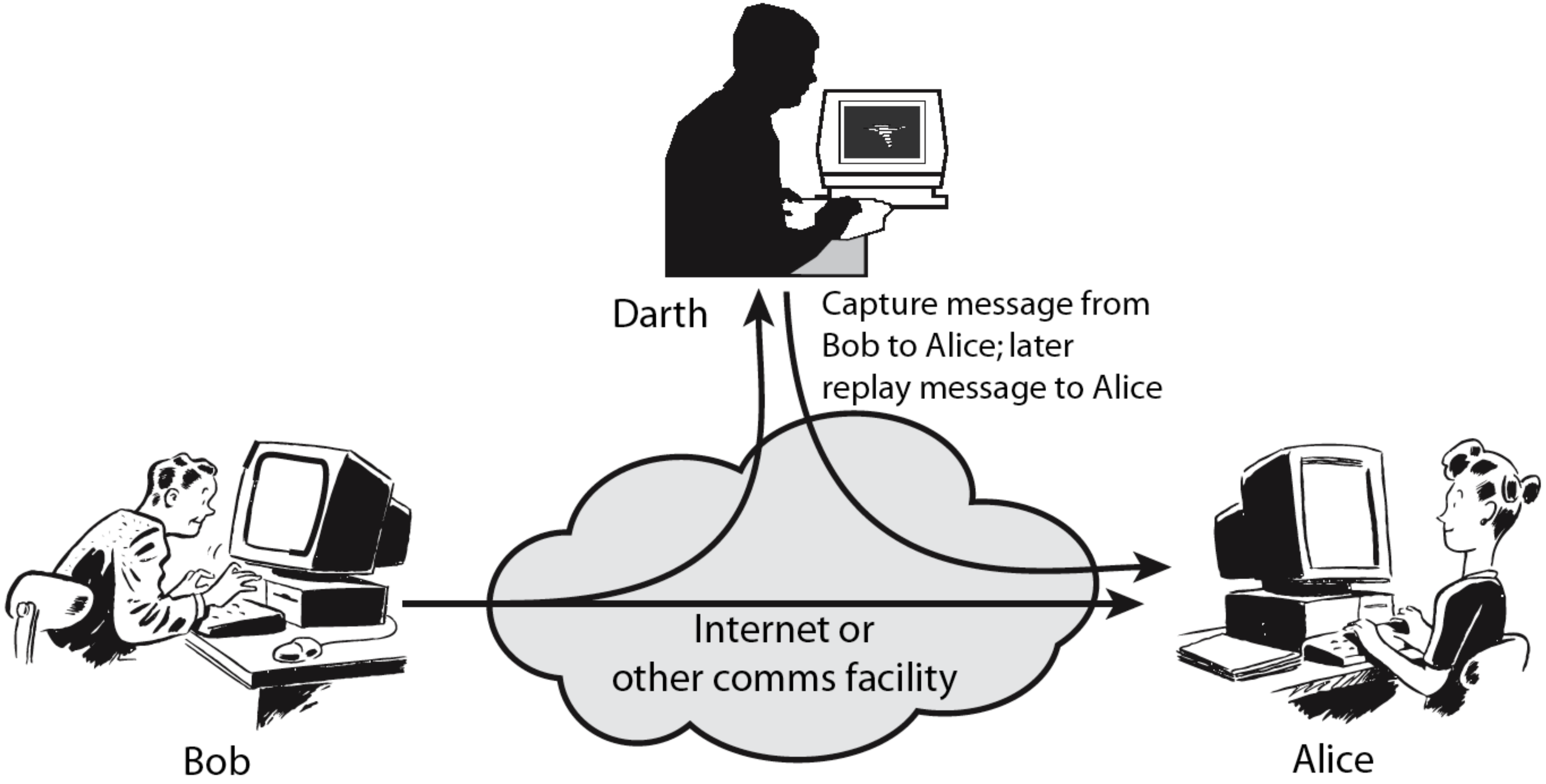
Attacks Threatening Availability

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

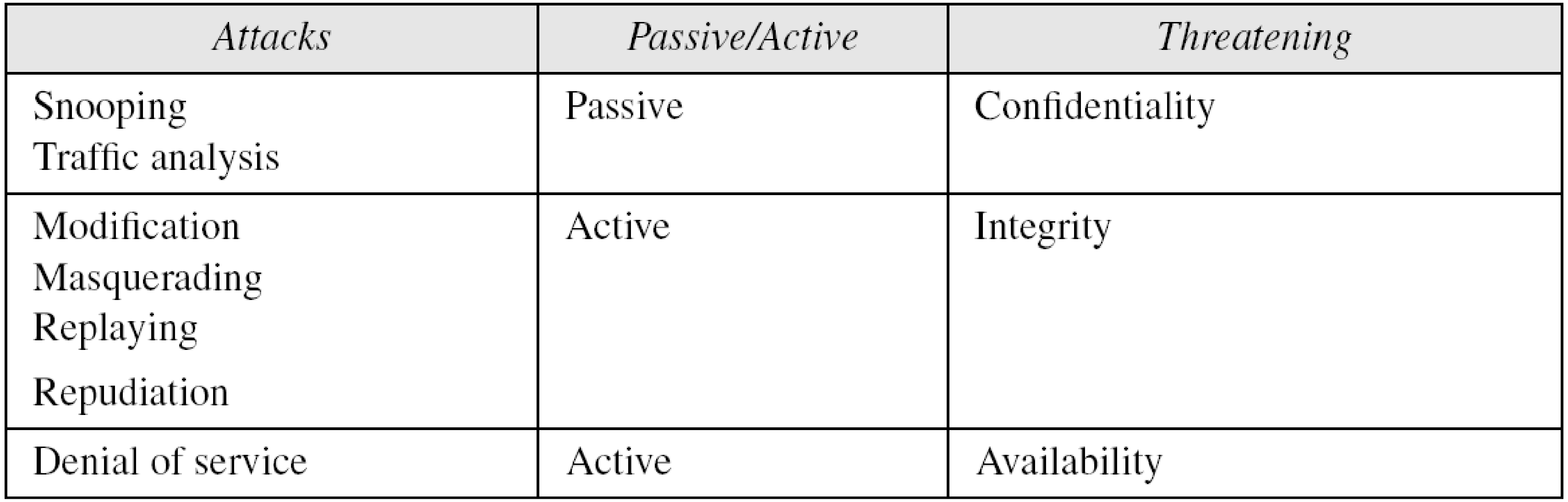
Passive Attacks



Active Attacks



Categorization of Passive and Active Attacks



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

SERVICES AND MECHANISMS

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..

Security Services

Security Mechanism

Relation between Services and Mechanisms

Security Attacks and Security Services

Security Attack : Any action that compromises the security of information owned by an organization.

Security Services : A service that enhances the security of the data processing systems and the information transfers of an organization. The services are more intended to counter security attacks and they make use of one or more security mechanism to provide the service.

Security Attacks

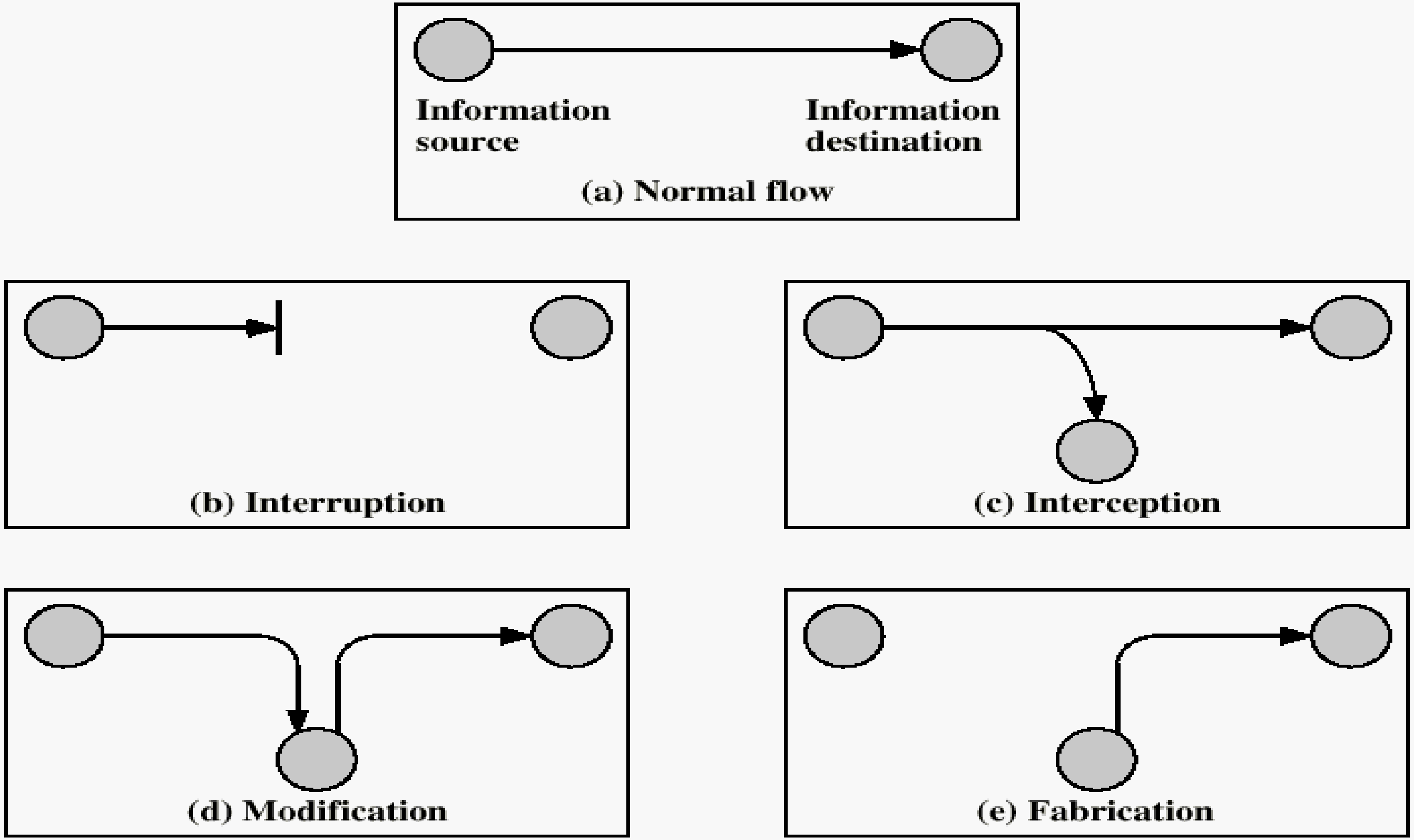
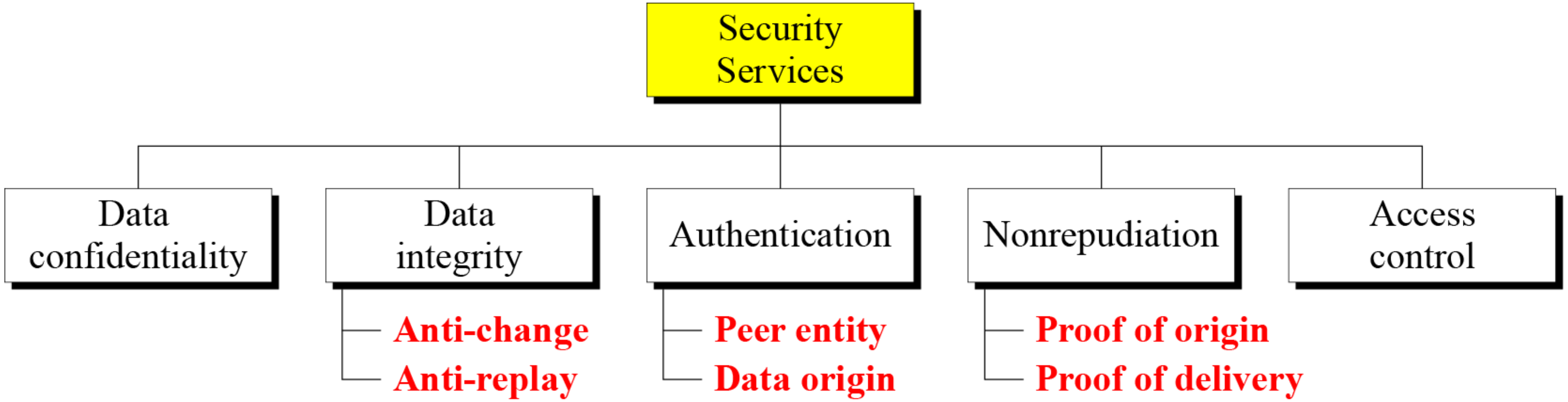


Figure 1.1 Security Threats

Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Security Services



Security Services

Data confidentiality

Data integrity

- Anti-change
- Anti-replay

Authentication

- Peer entity
- Data origin

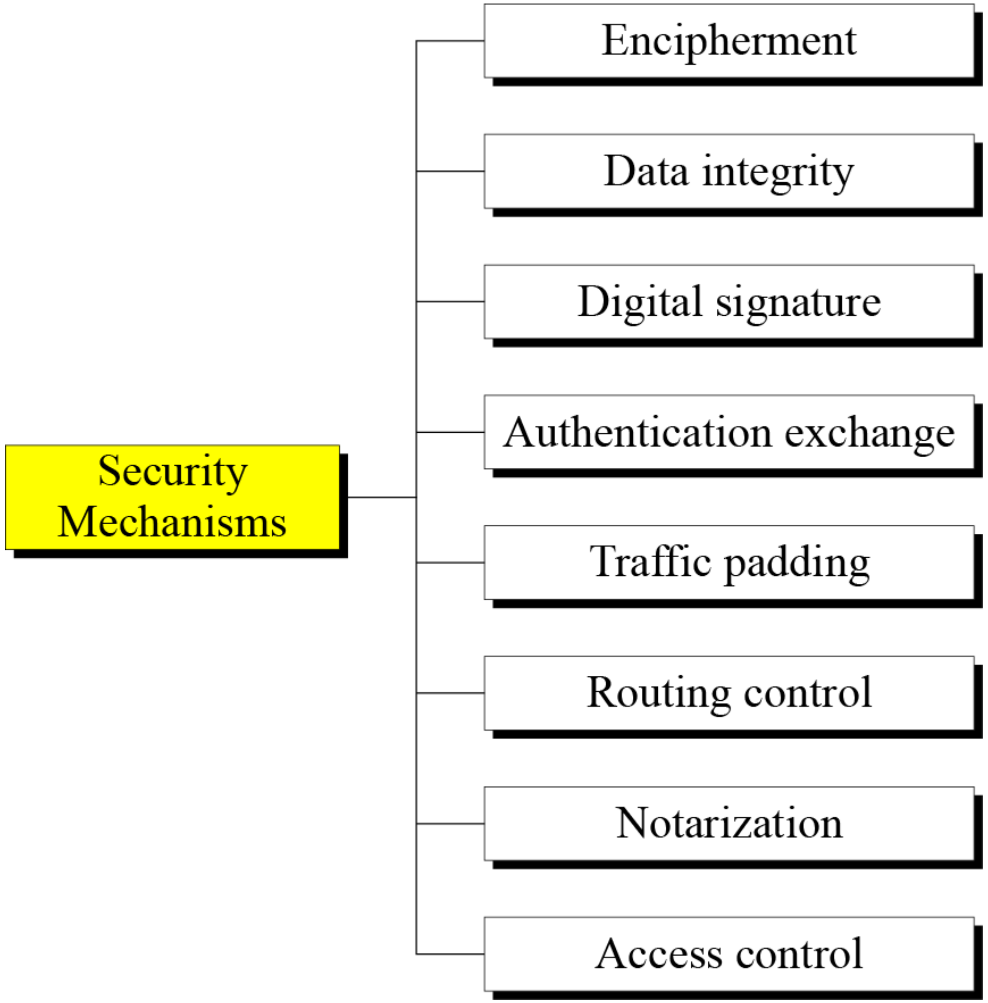
Nonrepudiation

- Proof of origin
- Proof of delivery

Access control

Security Mechanisms

Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.

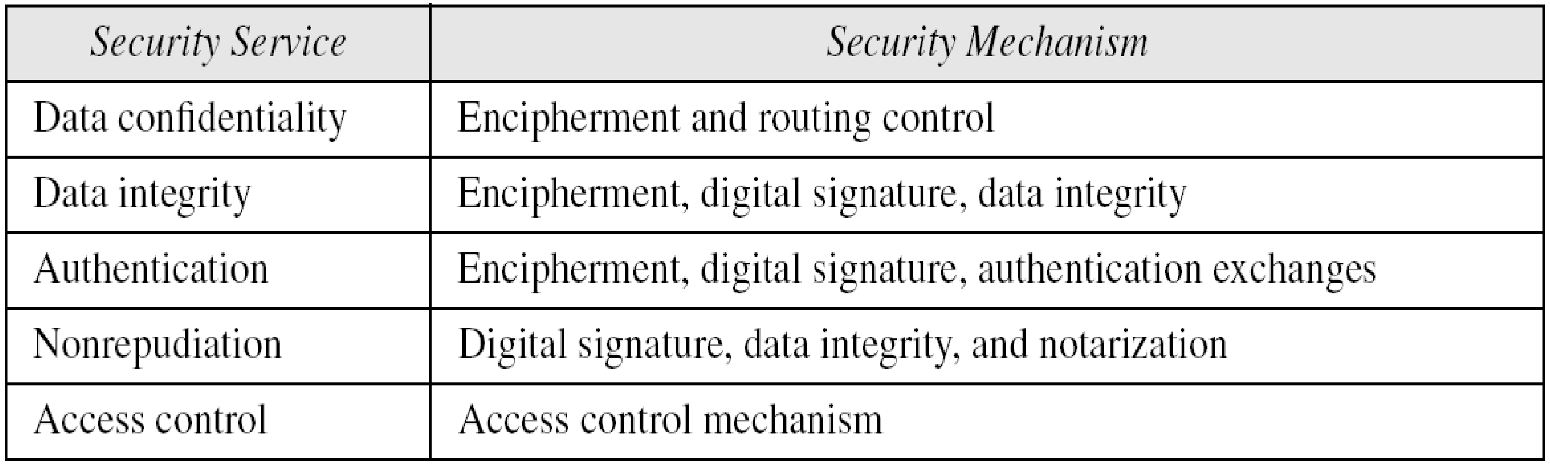


- **Notarization** means selecting a third party to control the communication between two entities. This can be done for example, to prevent repudiation.

Relation between Services and Mechanisms

Security Service: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.



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