Cryptography and Network Security
Introduction

Objectives

- To define three security goals
- To define security attacks that threaten security goals
- OSI Security Architecture
- To define security services and how they are related to the three security goals
- To define security mechanisms to provide security services
- To study Network security model

Background

- Traditionally security provided by physical and administrative mechanisms
- Information Security requirements have changed in recent times
- computer use requires automated tools to protect files and other stored information
- use of networks and communications links requires measures to protect data during transmission

Chapter 1 – Introduction

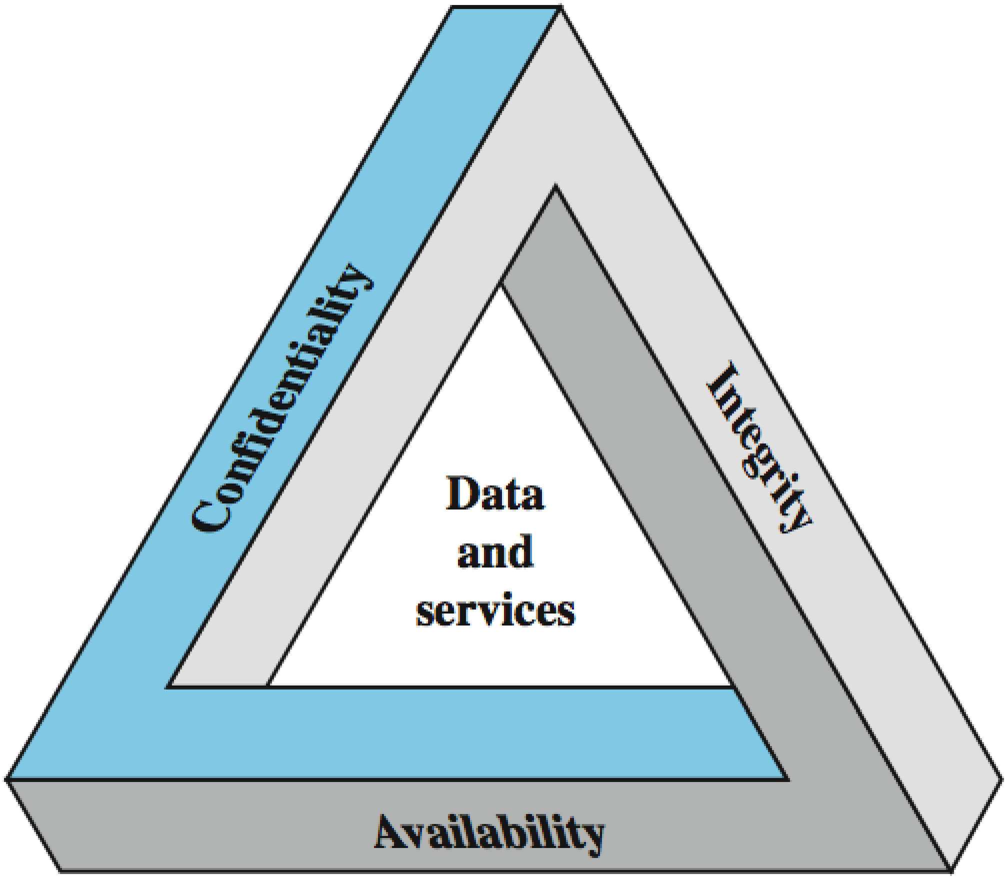
The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—*The Art of War*, Sun Tzu

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to prevent hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Key Security Goals



Key Security Goals (contd…)

To be secured, information need to be :

- Hidden from unauthorized access i.e. **Confidentiality**
- Protected from unauthorized change i.e. **Integrity**
- Available to an authorized entity when it is needed i.e. **Availability**

Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – authentication service

Levels of Impact

- can define 3 levels of impact from a security breach
  - Low
  - Moderate
  - High

Aspects of Information Security

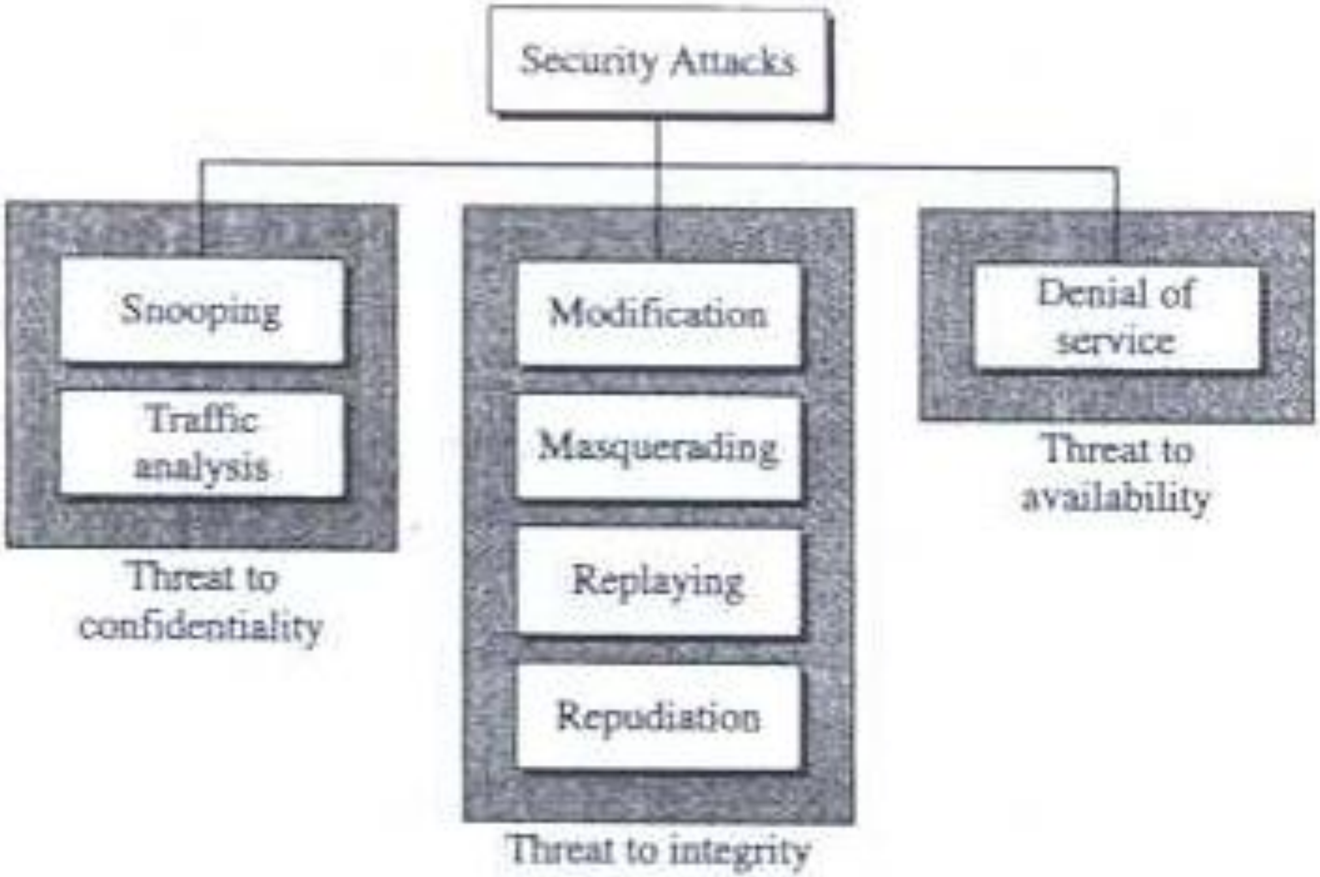
- 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**
- note terms
  - *threat* – a potential for violation of security
  - *attack* – an assault on system security, a deliberate attempt to evade security services

Cryptographic Attacks

Cryptographic attacks are of two types:

- **Cryptanalytic Attacks**: are combinations of statistical and algebraic techniques aimed at ascertaining the secret key of a cipher.
- **Non-cryptanalytic Attacks**: threaten three goals of security.

Taxonomy of attacks with relation to security goals



Attacks threatening Confidentiality

- **Snooping** : Unauthorized access to or interception of data
- **Traffic Analysis** : Monitoring online traffic

Attacks threatening Integrity

- **Modification** : modifies the information for own benefit
- **Masquerading** : impersonates somebody else
- **Replaying** : replaying copy of message sent by user earlier
- **Repudiation** : performed by one of the parties in the communication i.e. the sender or the receiver

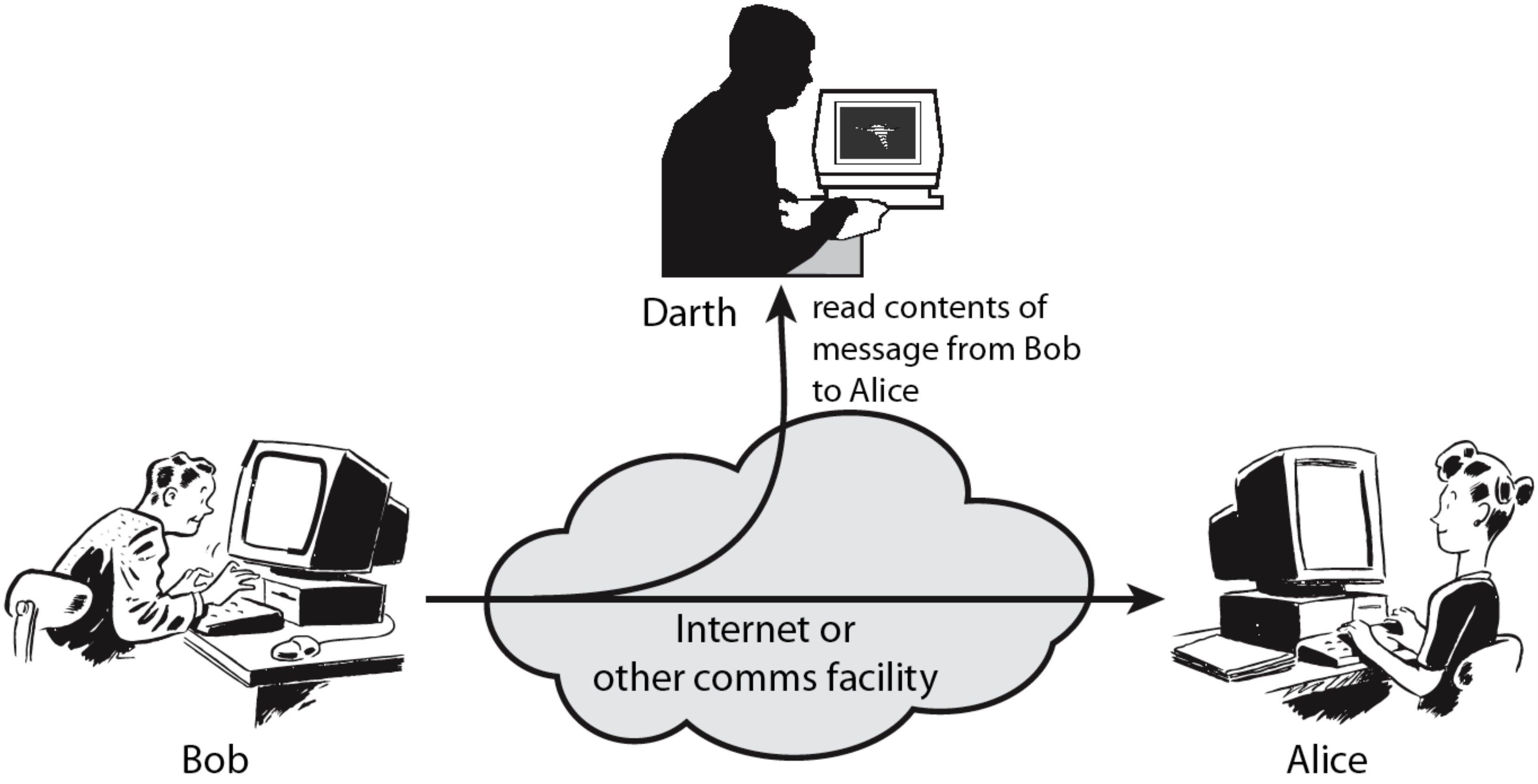
Attacks threatening Availability

- **Denial Of Service (DOS)** : slow down or totally interrupt the services of a system.

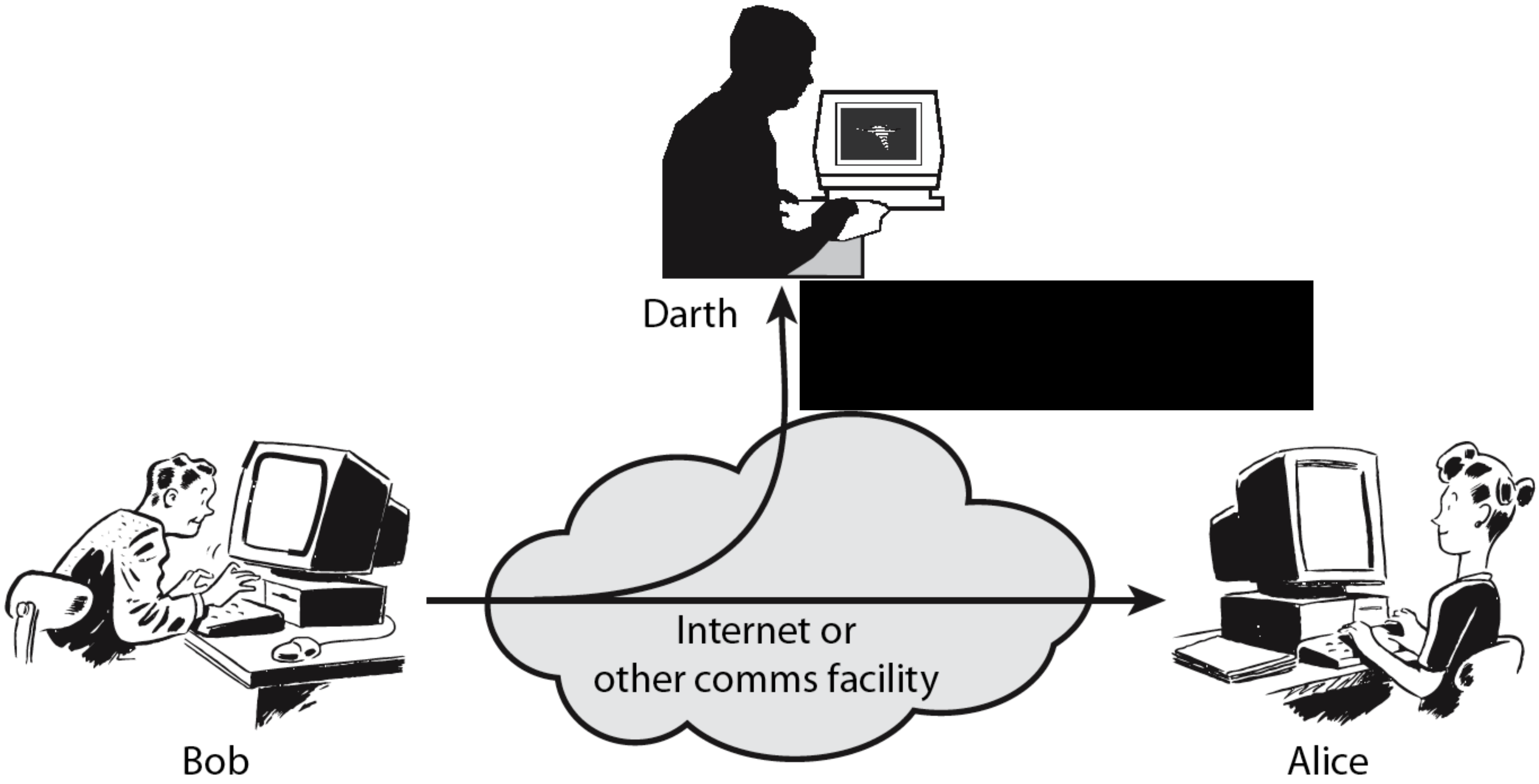
Generic types of Attacks

- Passive Attacks
  - *Passive attacks* are in the nature of eavesdropping on, or monitoring of, transmissions. They do not involve any alteration of the data.
- Active Attacks
  - Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service

Passive Attack - Interception

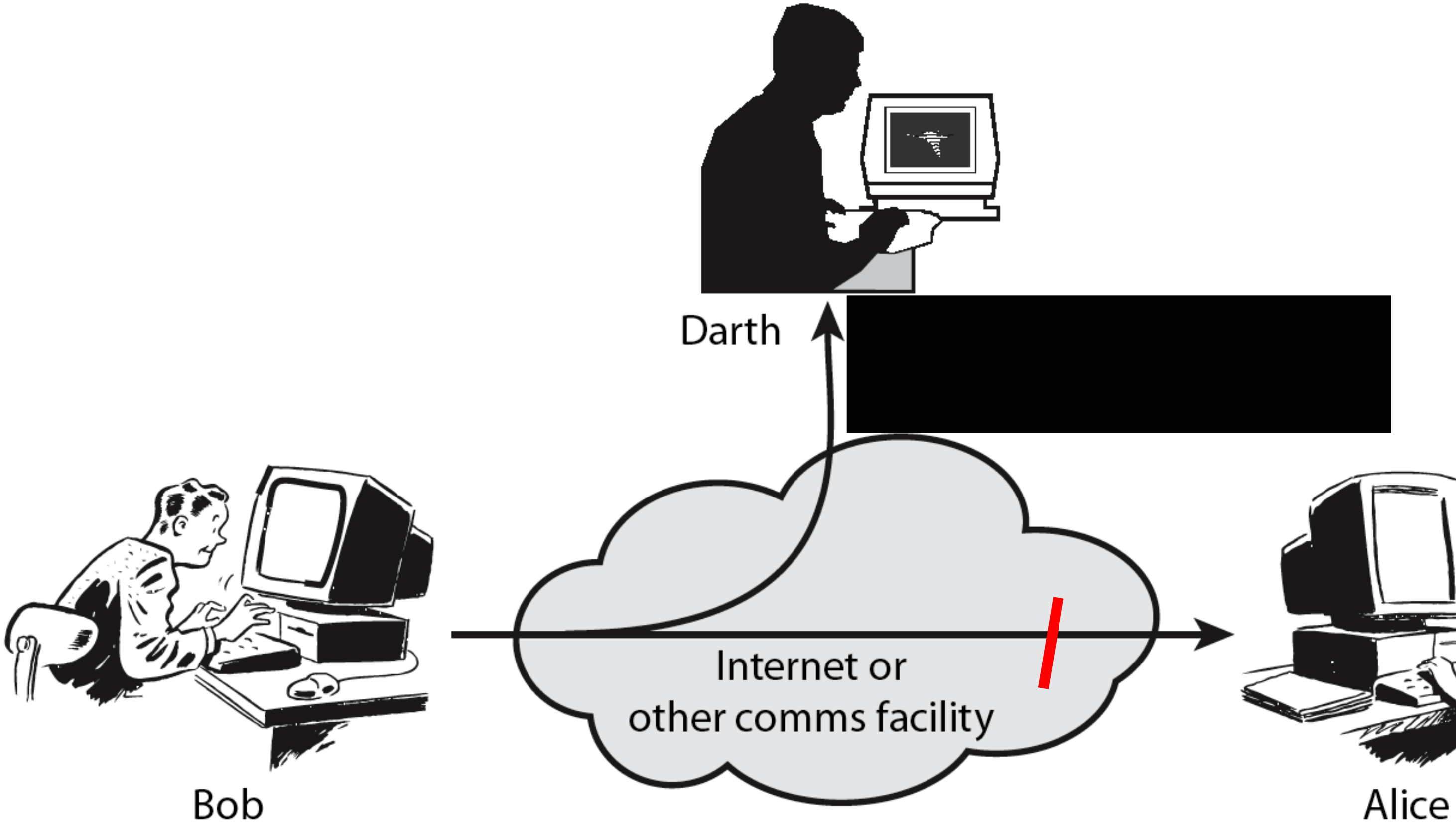

Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Passive Attack: Traffic Analysis

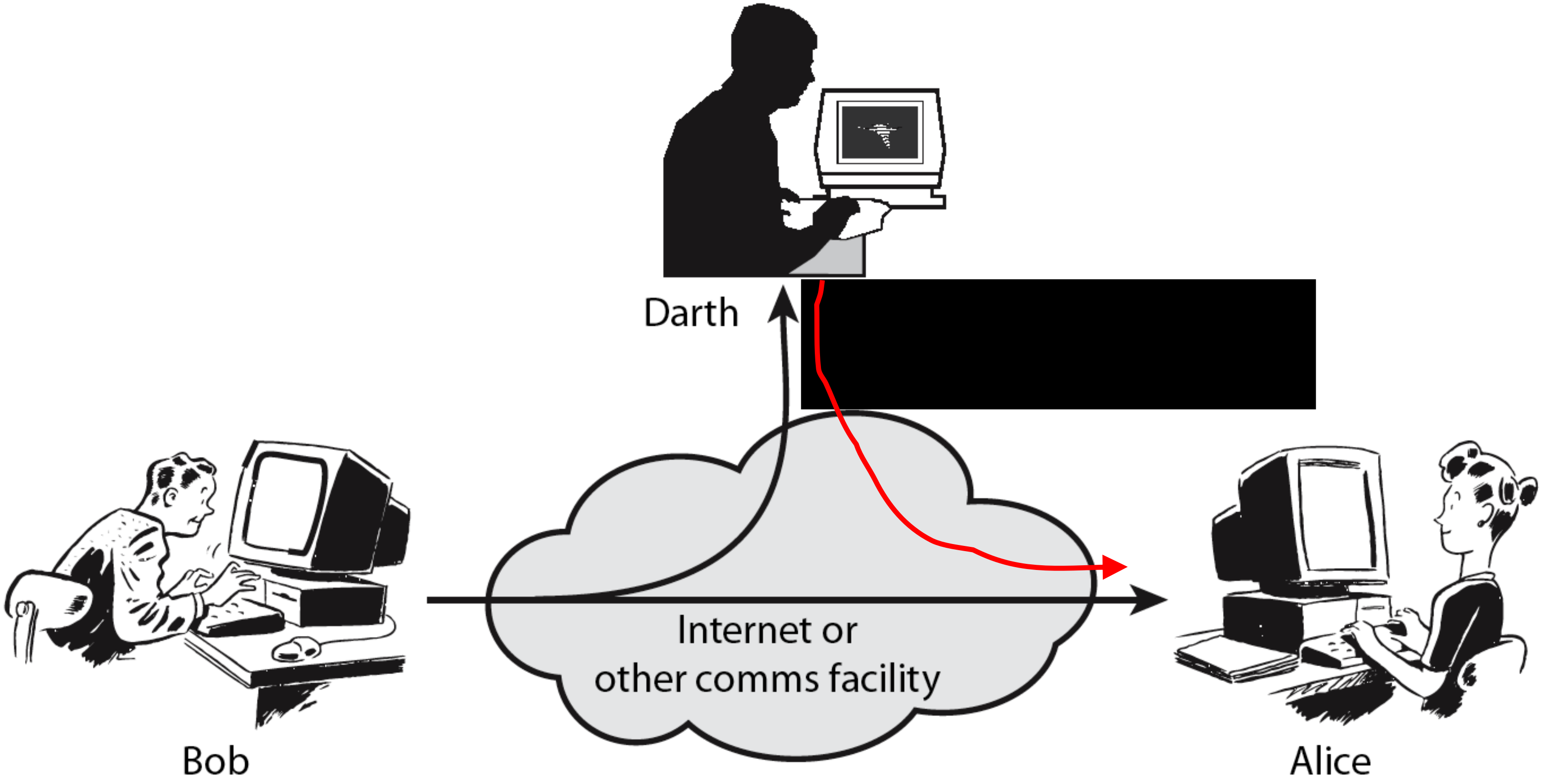


[redacted]

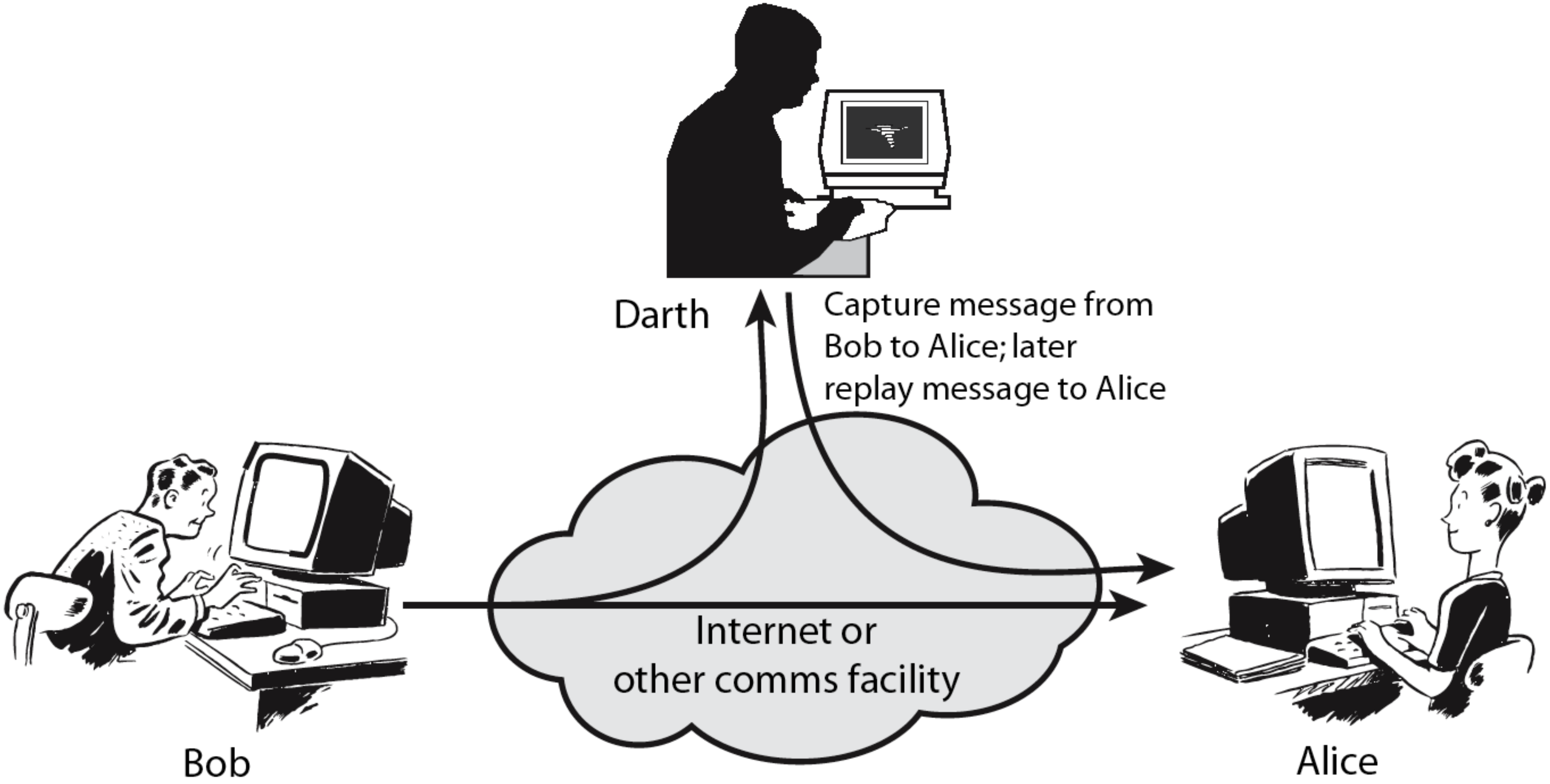
Active Attack: Interruption



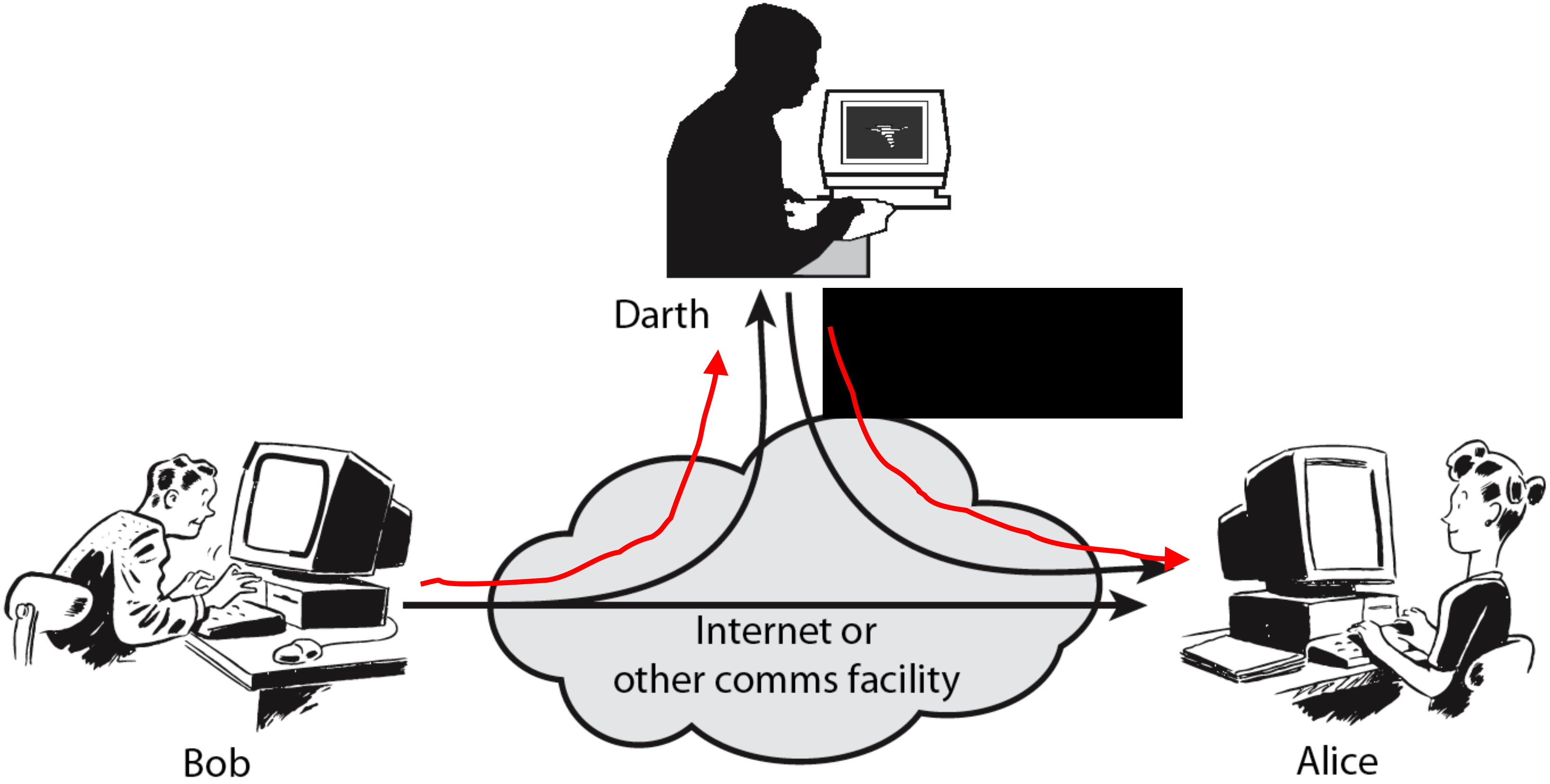
Active Attack: Fabrication



Active Attack: Replay


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

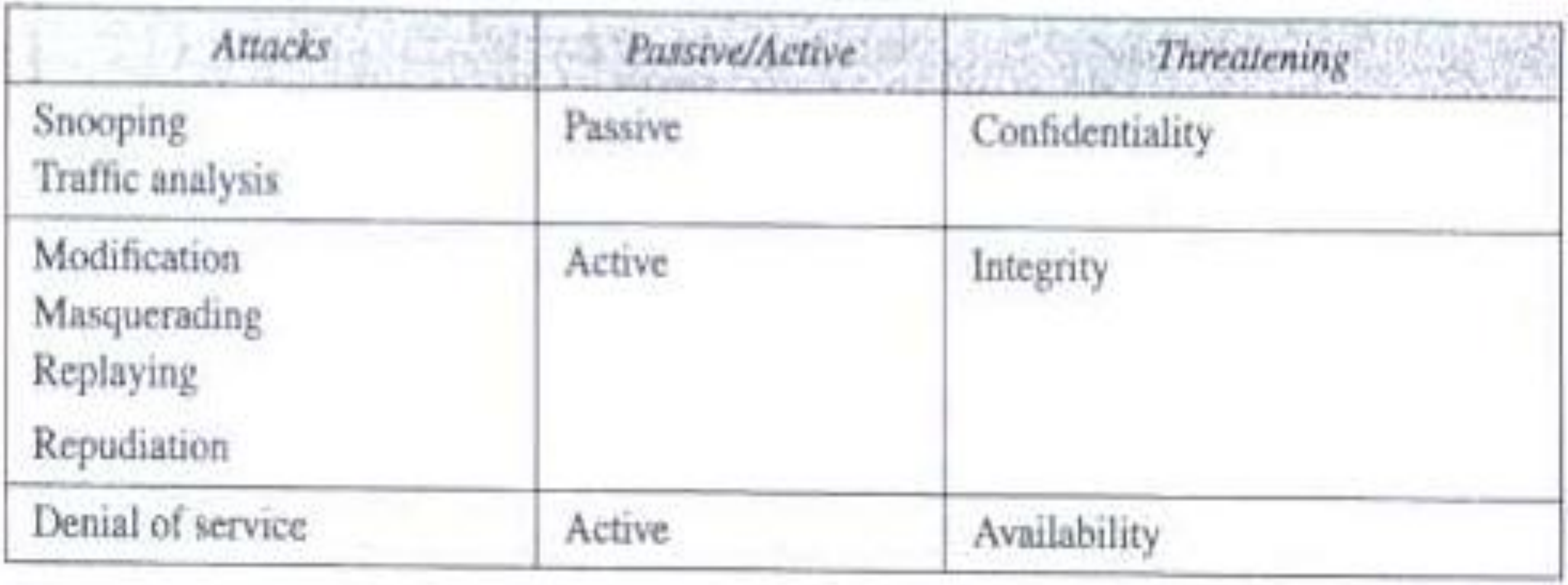
Active Attack: Modification



Handling Attacks

- Passive attacks – focus on Prevention
  - Easy to stop
  - Hard to detect
- Active attacks – focus on Detection and Recovery
  - Hard to stop
  - Easy to detect

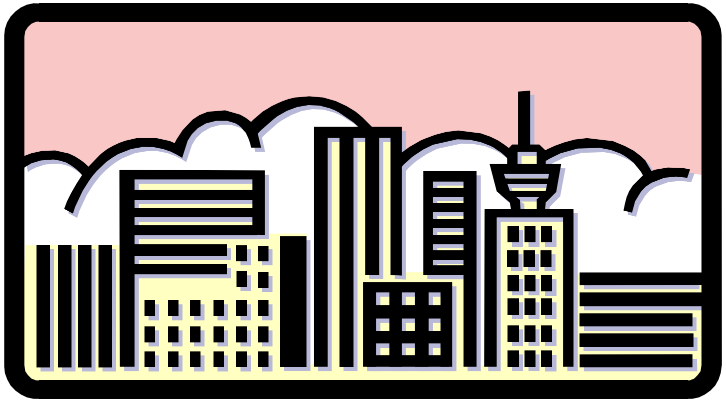
Categorization of passive and active attacks



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

OSI Security Architecture

- ITU-T X.800 "Security Architecture for OSI"
- defines a systematic way of defining and providing security requirements

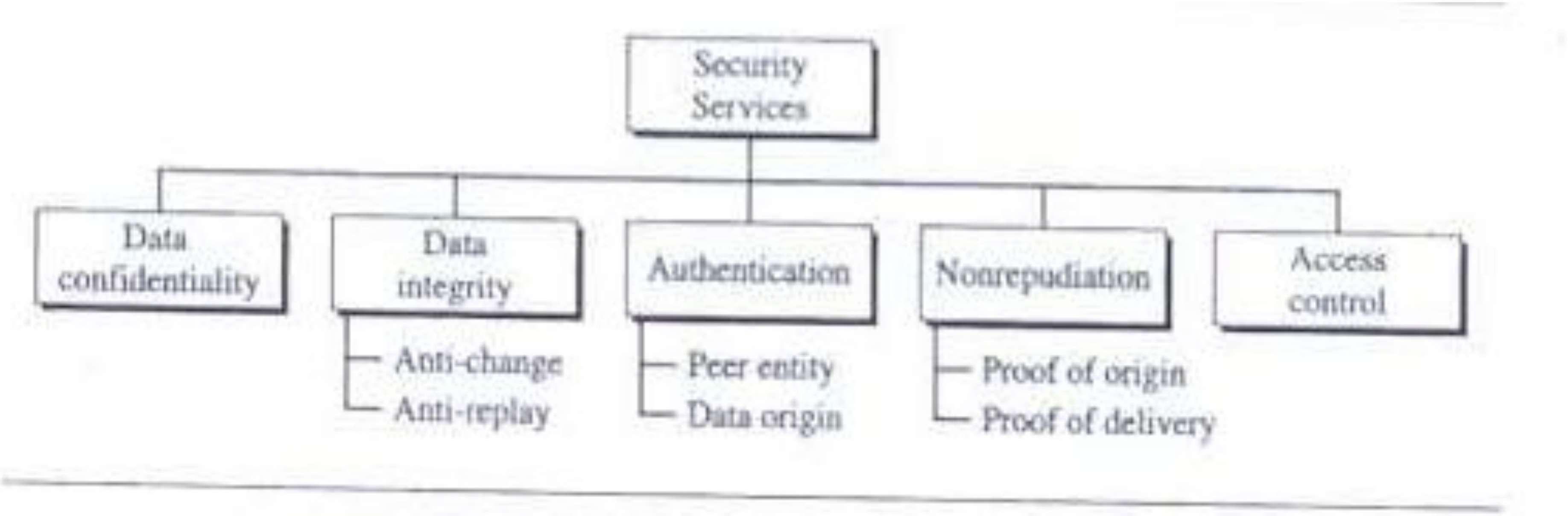


Services and Mechanisms

- ITU-T (X.800) provides some security services and some mechanisms to implement those services.
- Both are closely related

Security Services

- ITU-T (X.800) has defined five services related to goals and attacks we have studied.



Security Services (Contd…)

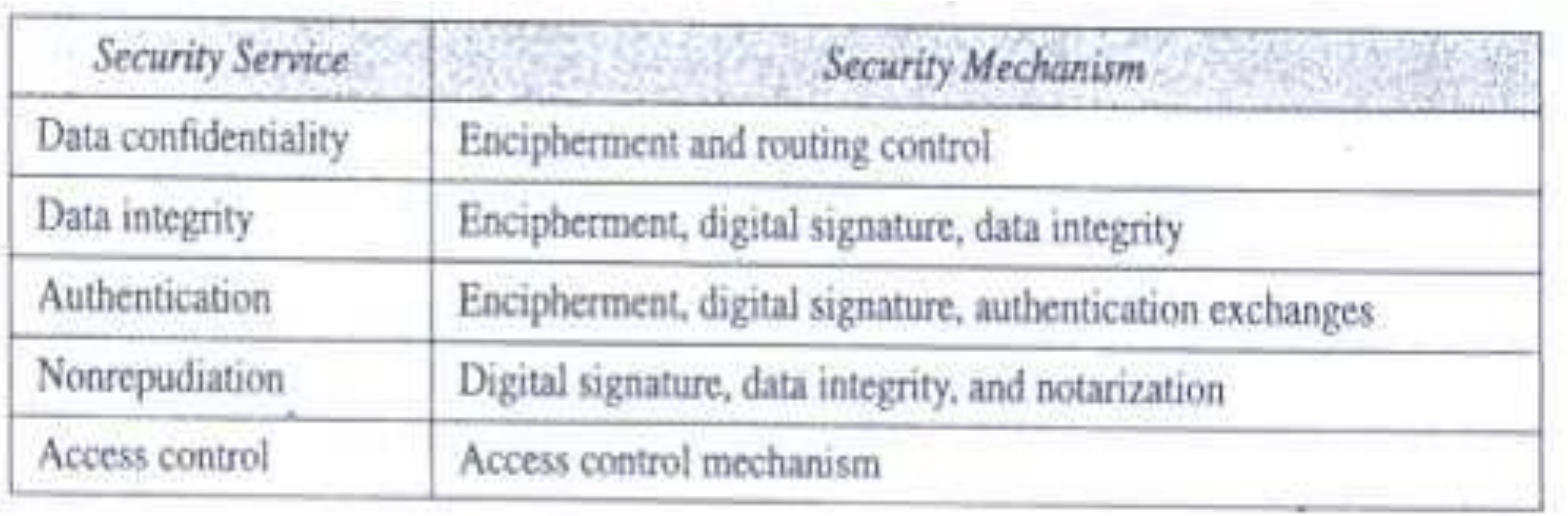
- Data Confidentiality
- Data Integrity: Anti-change, Anti-replay
- Authentication: peer entity, Data origin
- Nonrepudiation: proof of origin, proof of delivery
- Access Control

Security Mechanisms

ITU-T (X.800) recommends some mechanisms to provide the security services that we discussed.

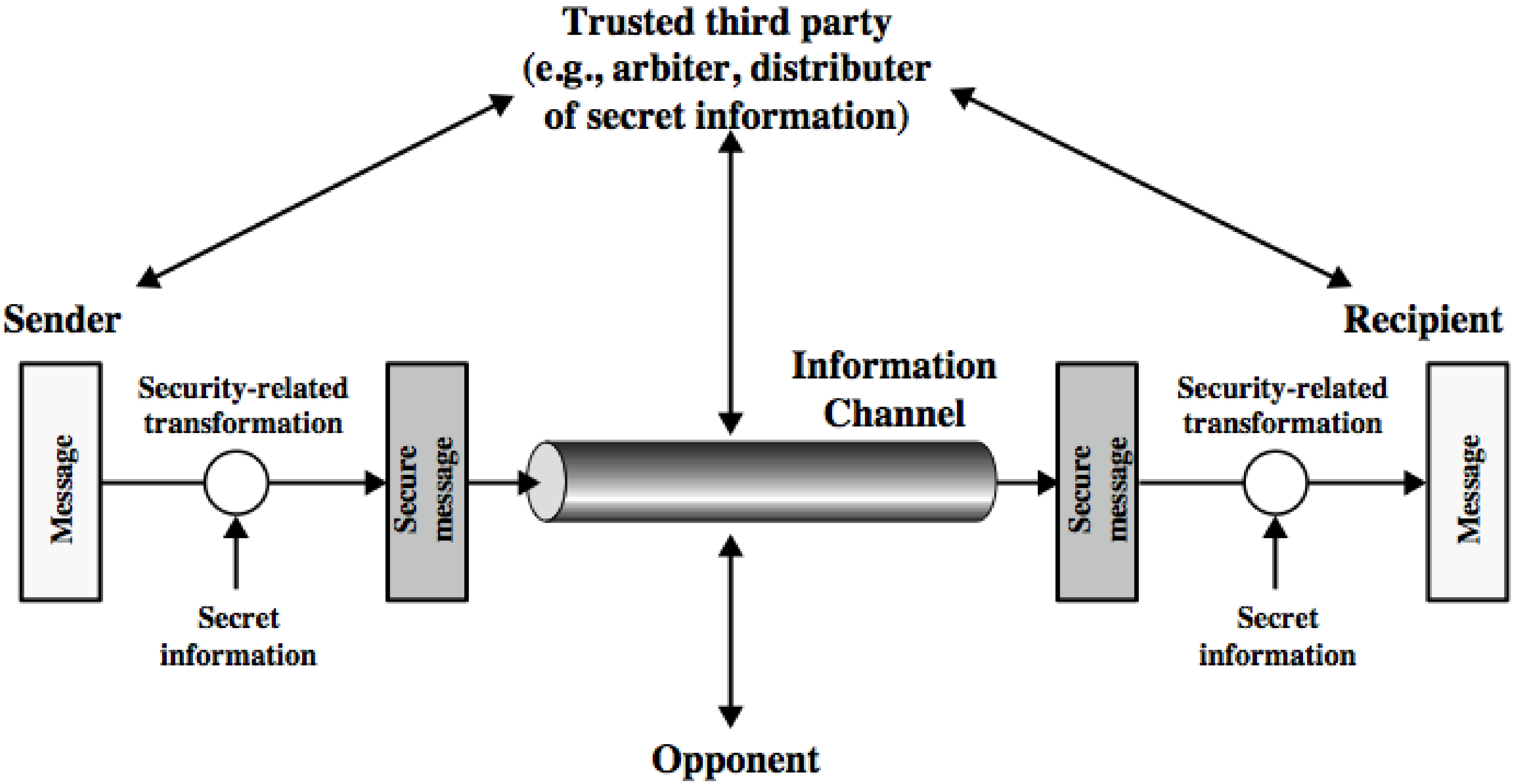
- Encipherment
- Data Integrity
- Digital Signature
- Authentication Exchange
- Traffic padding
- Routing Control
- Notarization
- Access Control

Relation Between 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

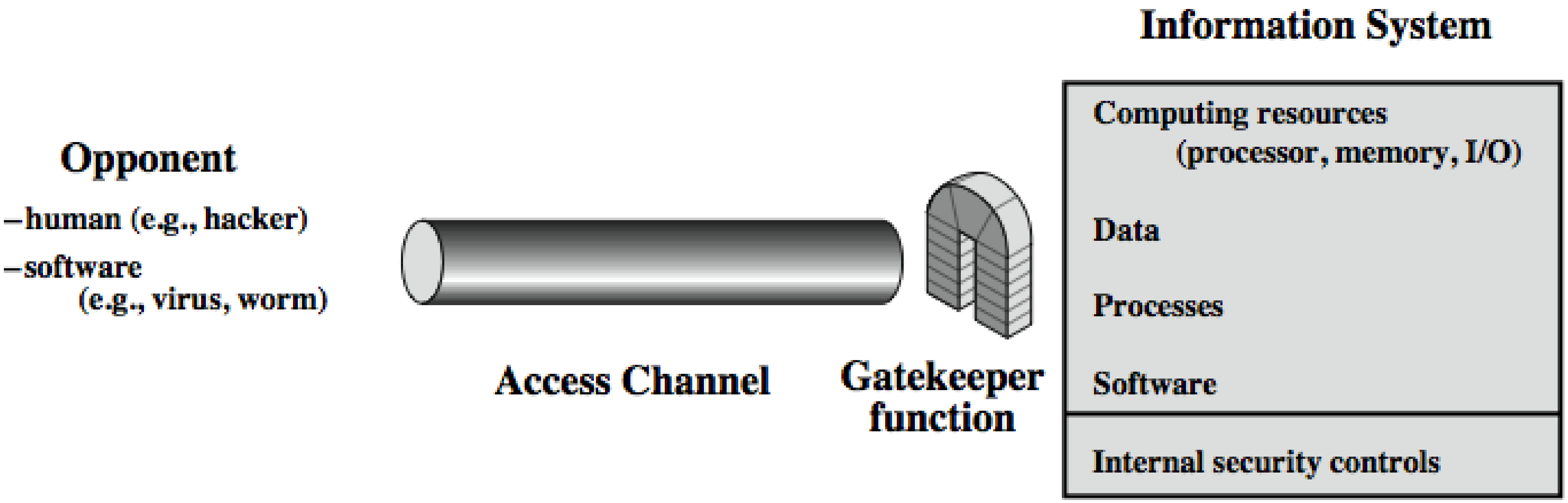
Model for Network Security



Model for Network Security

- 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



Information System

Computing resources
(processor, memory, I/O)

Data

Processes

Software

Internal security controls

Opponent

–human (e.g., hacker)

–software
(e.g., virus, worm)

Access Channel

Gatekeeper function

Summary

- security Goals:
  - confidentiality, integrity, availability
- security attacks, services, mechanisms
- OSI X.800 security architecture
- models for network (access) security

References

1. “Cryptography and Network Security”, 5/e, by William Stallings
2. “Cryptography and Network Security”, 2/e, by Behrouz A. Forouzan, Debdeep Mukhopadhyay