OSI SECURITY ARCHITECTURE

INTERNATIONAL STANDARD

ITU-T Recommendation X.800, Security Architecture for OSI defines systematic way to

- defining the requirements for security
- characterizing the approaches to satisfying those requirements

THE OSI SECURITY ARCHITECTURE FOCUSES ON SECURITY ATTACKS, MECHANISMS, AND SERVICES.

- **Security attack:** Any action that compromises the security of information owned by an organization.

- **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. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

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.

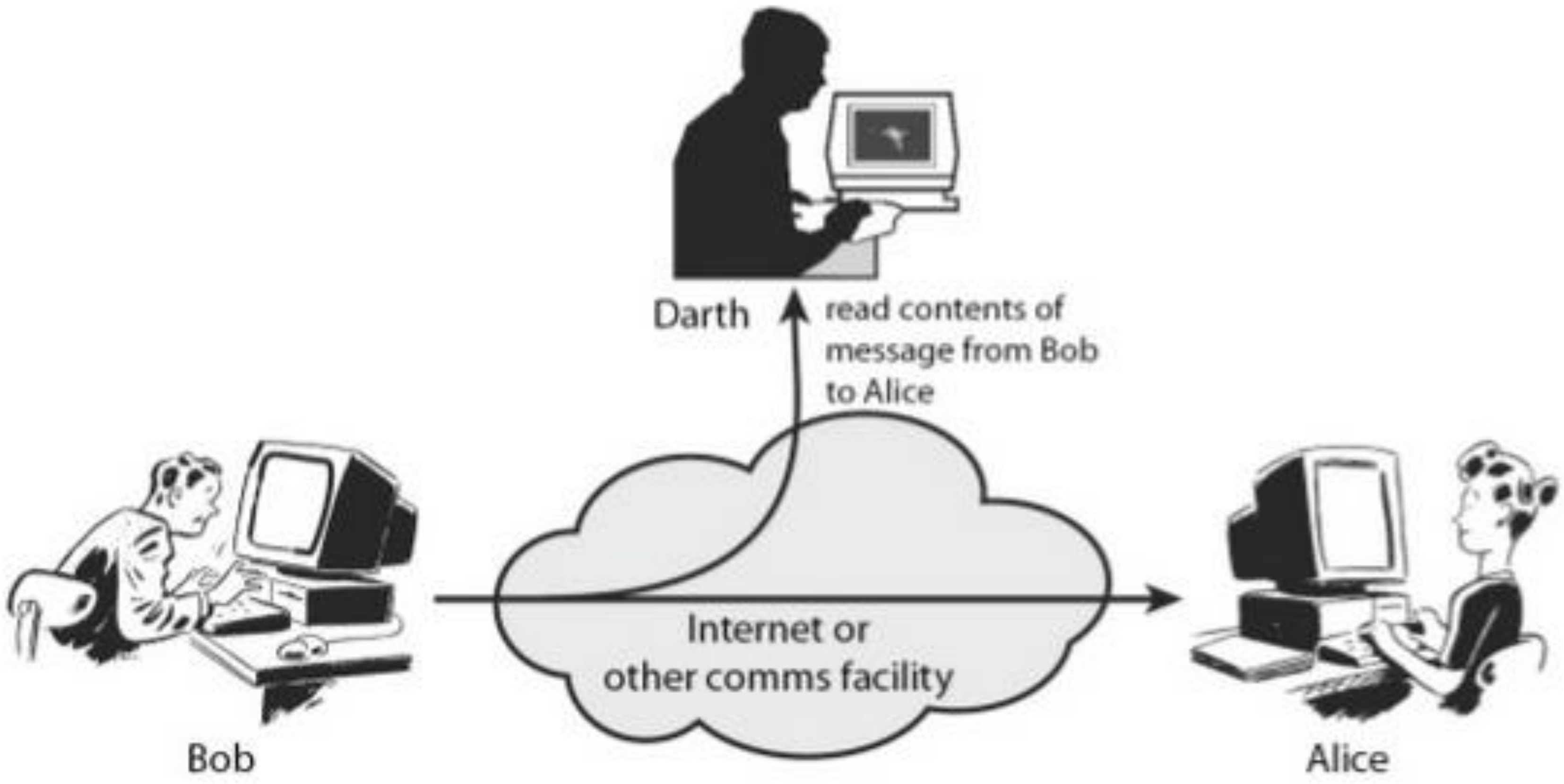
  Passive Attack

  Active Attack

PASSIVE ATTACKS

- Passive attacks are in the nature of monitoring transmissions.
- The goal of the opponent is to obtain information that is being transmitted.
- A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- Two types of passive attacks
    - Release of message contents
    - Traffic analysis

Passive Attacks


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

- Passive attacks are very difficult to detect, because they do not involve any alteration of the data.

- It is feasible to prevent the success of these attacks, usually by means of encryption.

- Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

ACTIVE ATTACKS

- Active attacks involve some modification of the data stream or the creation of a false stream
- It can be subdivided into four categories:

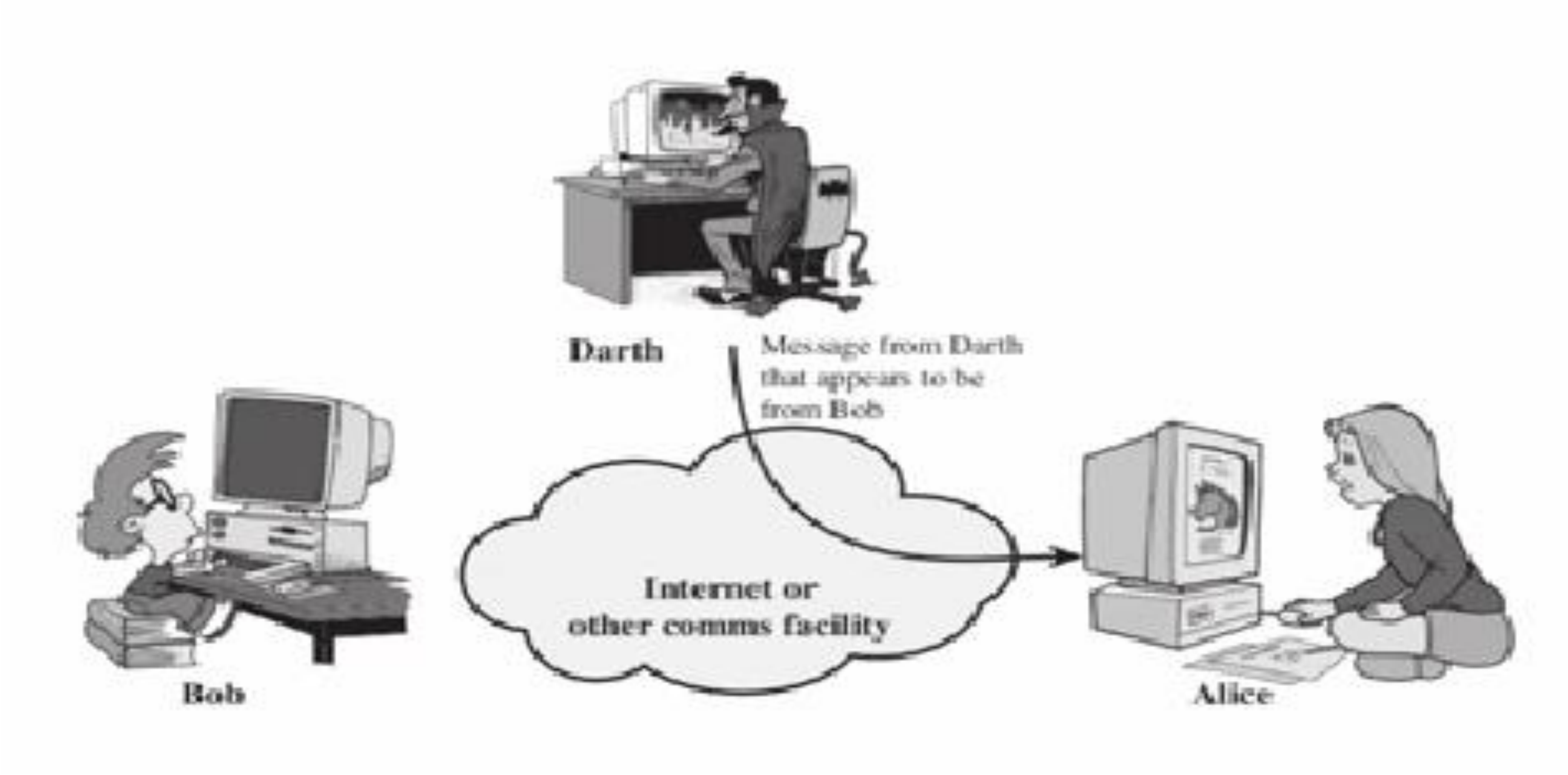
  Masquerade

  Replay

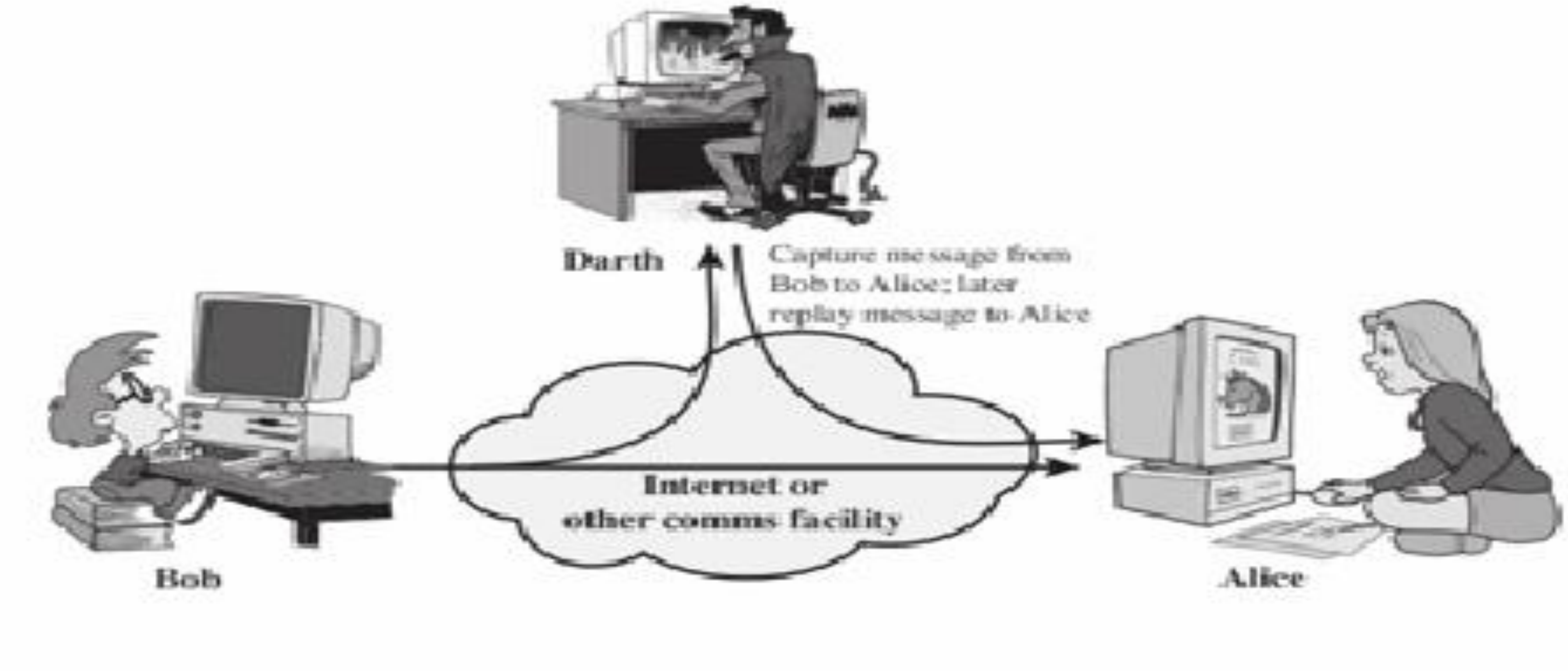
  Modification of messages

  Denial of service

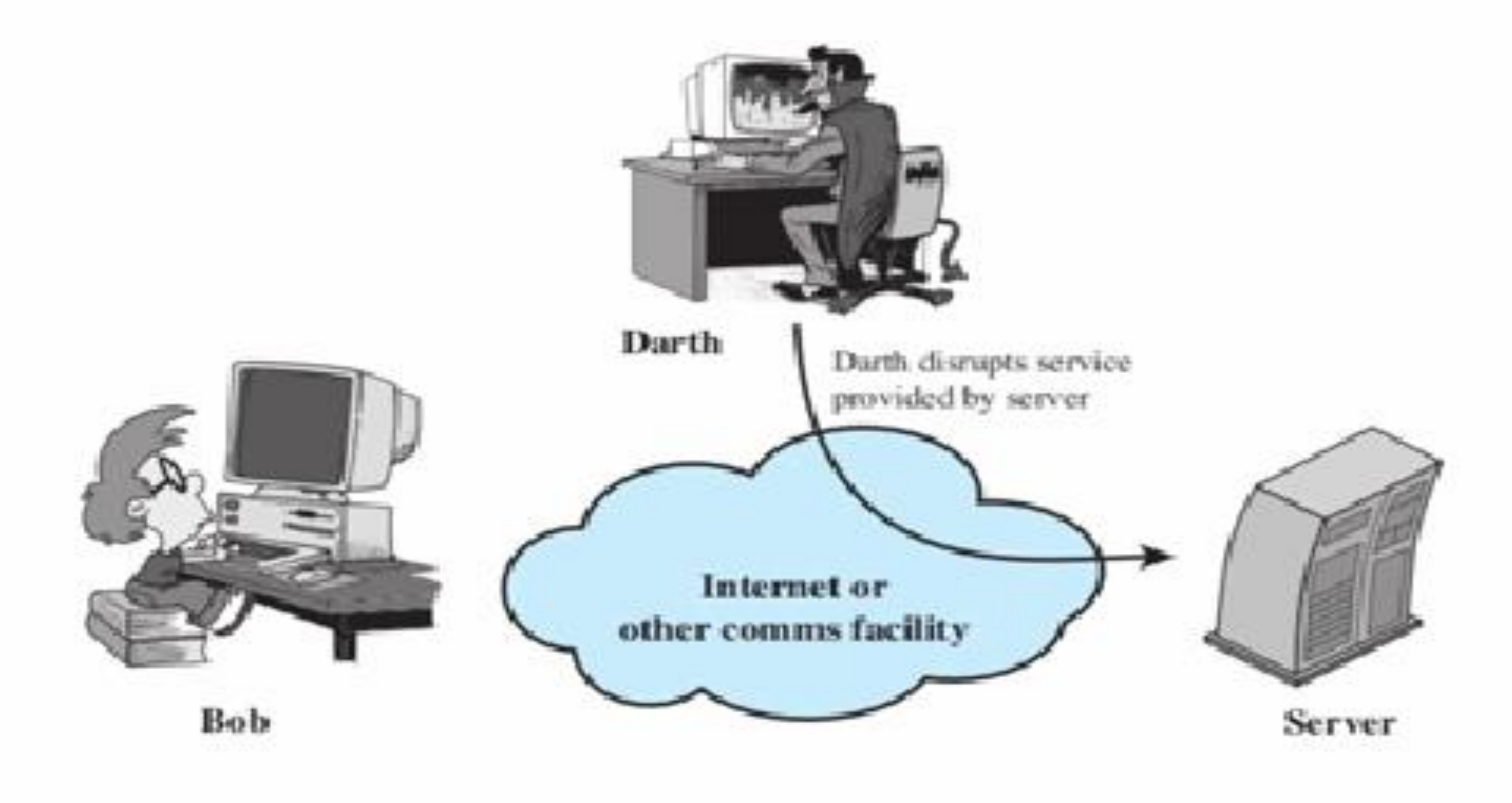
Masquerade Attack


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

Replay and Modify Attack


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

Denial of Service


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

SECURITY SERVICES

- Service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

- A processing or communication service that is provided by a system to give a specific kind of protection to system resources.

- Security services implement security policies and are implemented by security mechanisms.

Five Categories of Services

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation

SECURITY MECHANISMS

- A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted.

- Irreversible encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications