Lecture 1

Introduction

- In early days, not much emphasis was given to security.
- The security of information was completely under the control of an organization.
- Information security was not a major issue.

- Growing computer use requires automated tools to protect information.
- Use of networks requires measures to protect data during transmission.
- Information security gained more prominence.
- Computer security
- Internet and network security

Security Goals

- Confidentiality
- Integrity
- Availability

Key Aspects

- Security Attack
- Security Services
- Security Mechanisms

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

- Security service – A process that enhances the security of information transfer of an organization.

- Security mechanism – A process that is designed to detect or recover from a security attack.

Security attacks

- Classified into two:
  - Passive attack
  - Active attack

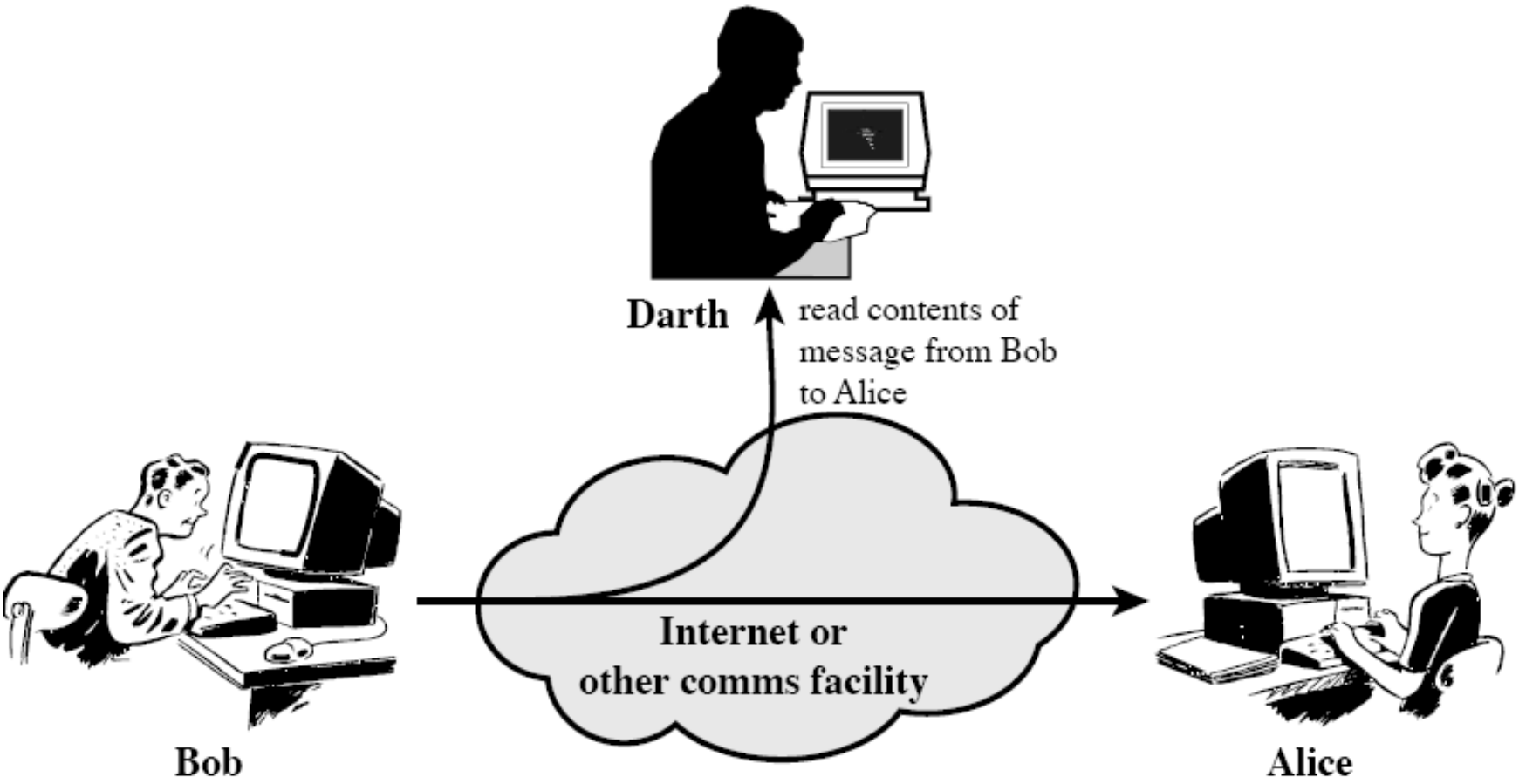
Passive attack

- Attempts to learn or make use of information that is in transit, but does not attempt to make any modification to the information.
- Harder to detect.
- Emphasis is on prevention, rather than detection or correction.

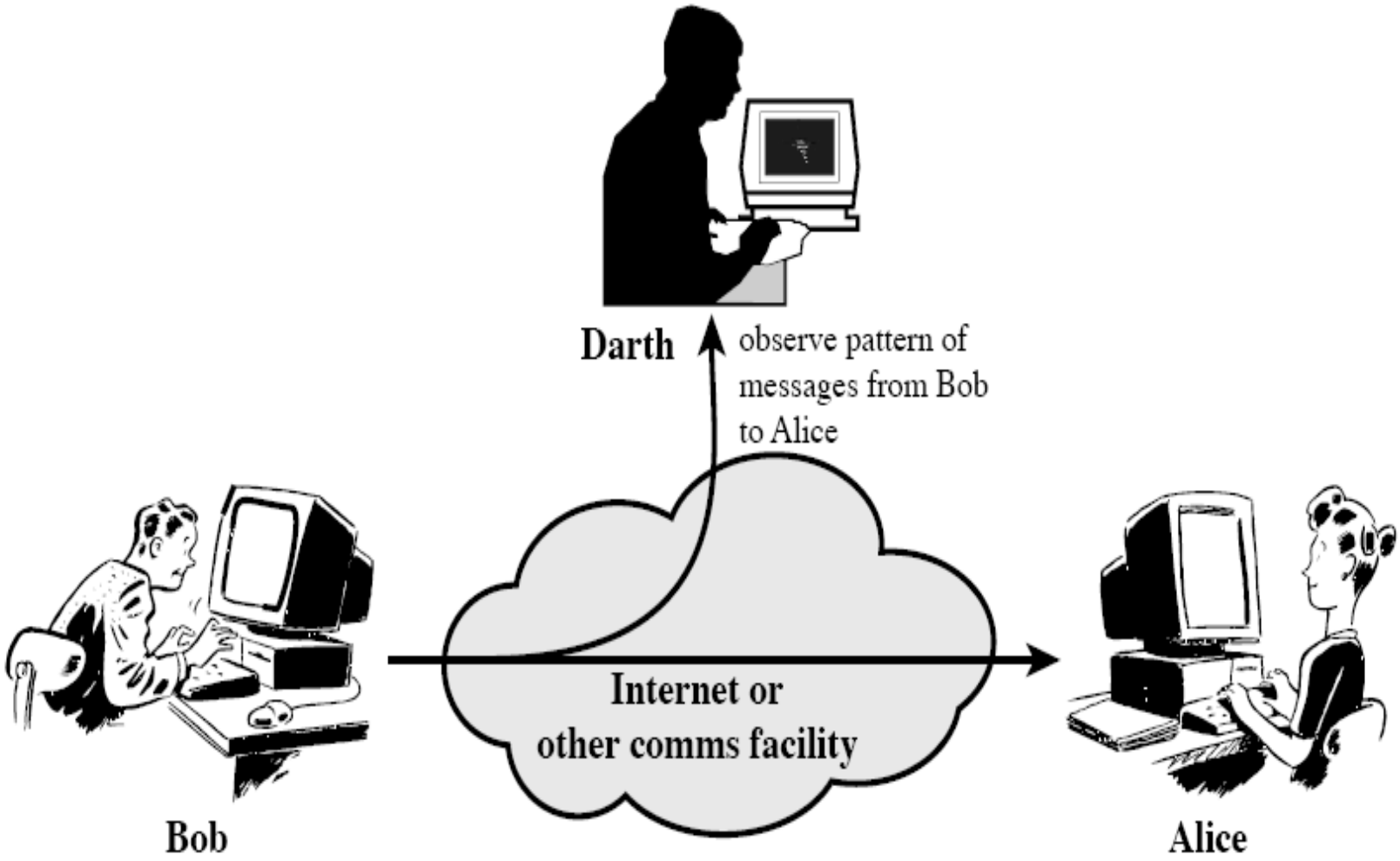
Passive attack

- Snooping
- Traffic analysis
- These two attacks threaten confidentiality

Snooping


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

Traffic analysis



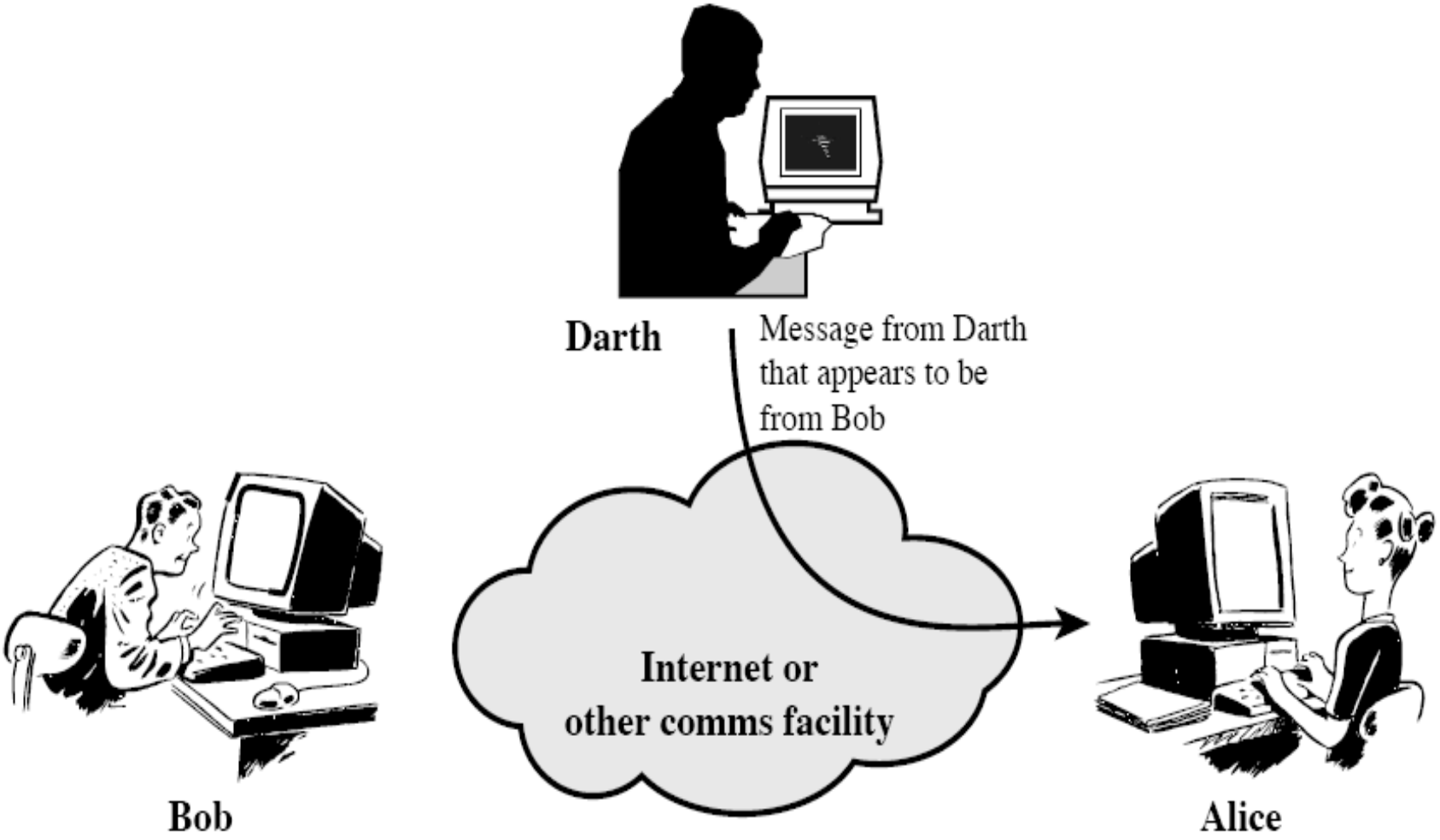
Active attack

- Attempts to alter the information that is transmitted.
- Cannot be prevented easily.
- Can be detected with some effort & attempts can be made to recover from the attack .

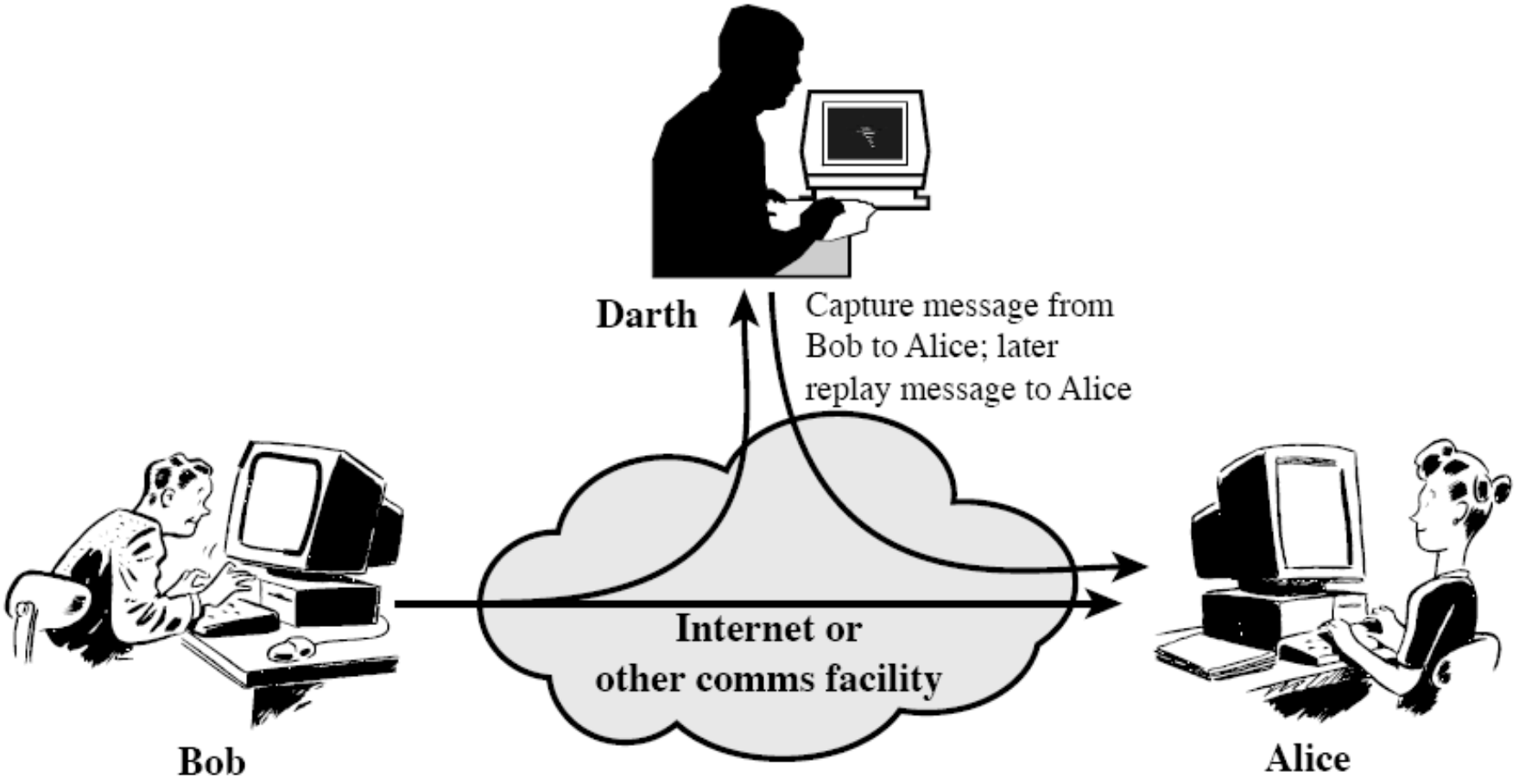
Active attack

- Masquerade
- Replay
- Modification of messages
- Repudiation
- Denial of Service

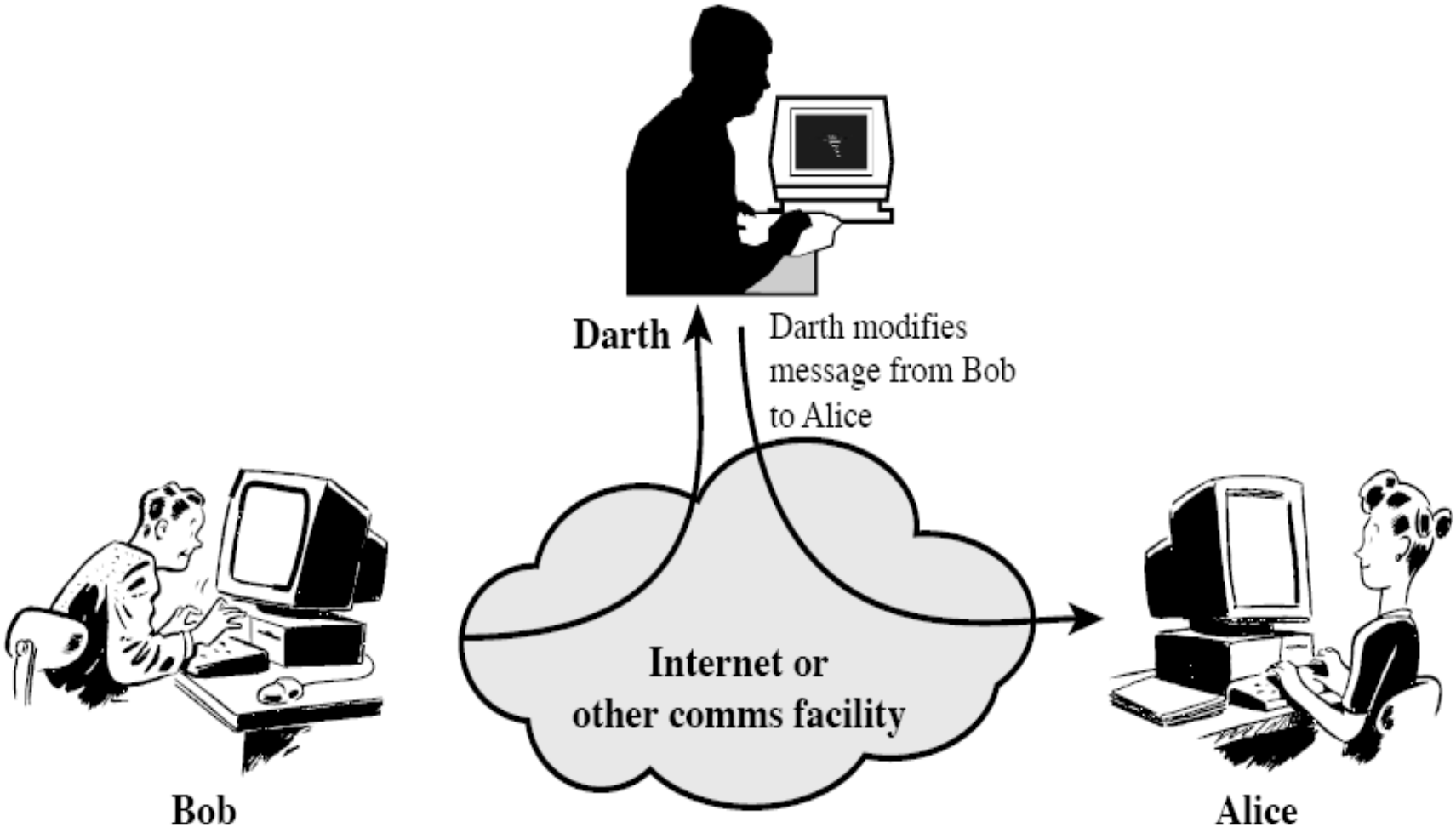
Masquerade


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

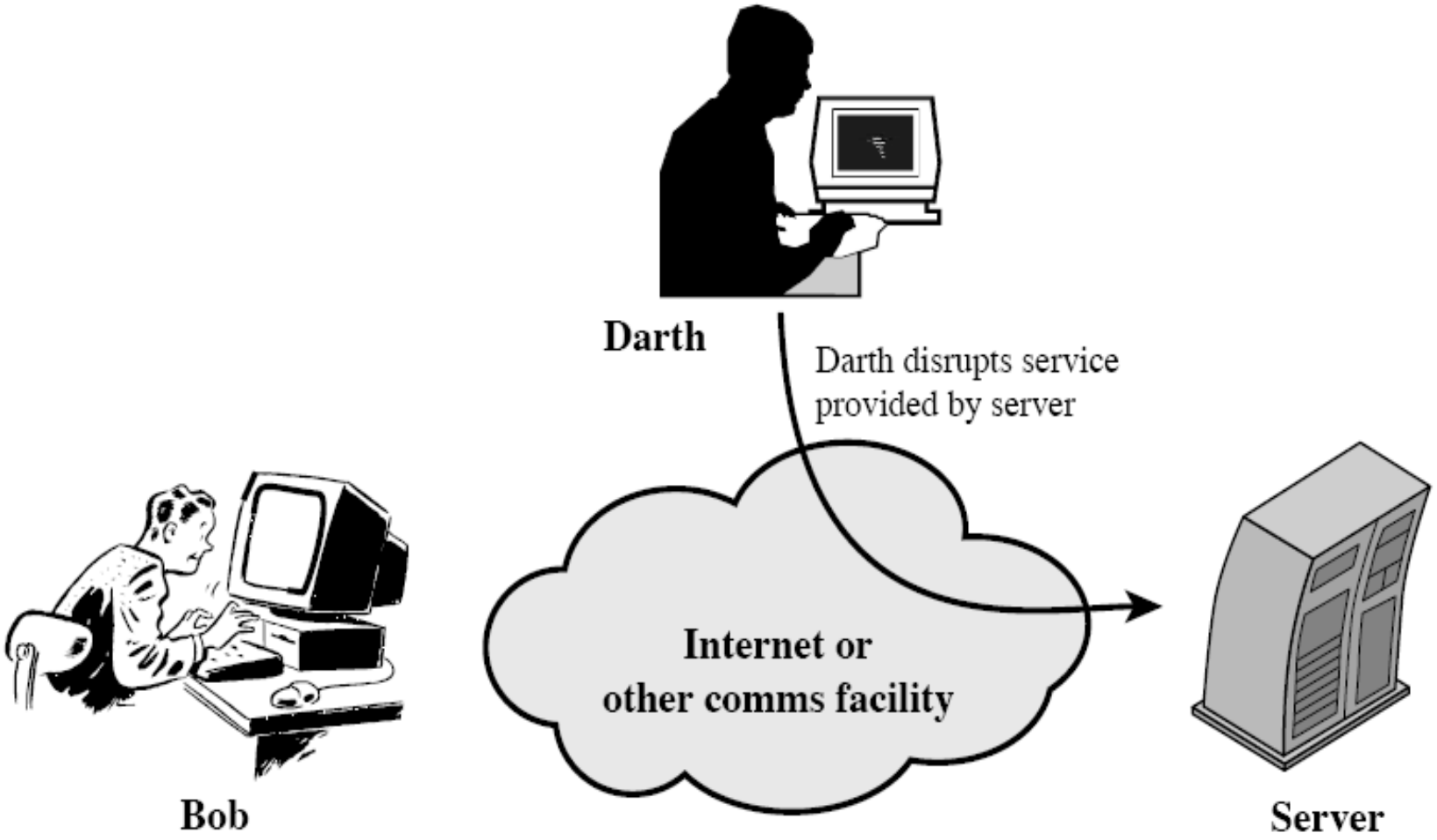
Replay


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

Modification of messages



Denial of service



Security Services

- Data Confidentiality – It is designed to protect data from disclosure attack.

- Data Integrity – It is designed to protect data from modification, insertion ,deletion,and replaying.
- Authentication – Ensures that the communicating entity is the one that it claims to be.

- Non-repudiation – Ensures protection against denial by one of the parties in a communication.

- Access control – Ensures prevention of unauthorized use of a resource. It determines ***who*** should be able to access ***what***.

Security Mechanisms

- Encipherment – Use of mathematical algorithms to transform data into a form that is not readily intelligible.

- Digital signature – Sender can digitally sign the information and a receiver can verify it.

- Traffic padding – Insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

- Access control – Variety of mechanisms that enforce access rights to resources.
- Data integrity – Variety of mechanisms used to assure the integrity of a data unit.
- Notarization – Use of a trusted third party to control the communication between two entities.

- Authentication Exchange – Two parties can exchange information to prove each other that they are communicating.

- Routing Control – Enables selection or change of available communication channel .