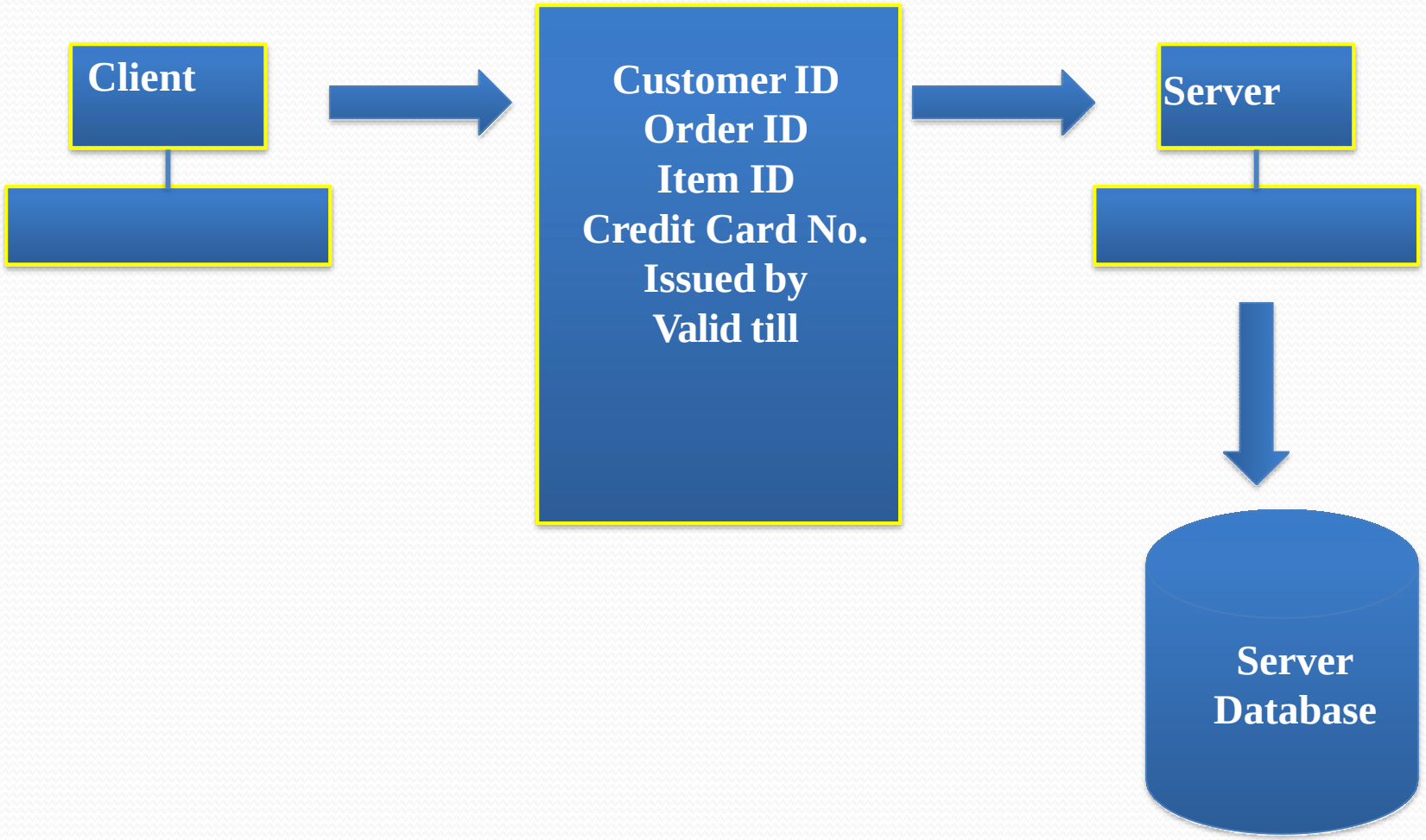
Cryptography
&
Network Security

Some Basic Terminology

- **Plaintext -** original message
- **Ciphertext -** coded message
- **Cipher -** algorithm for transforming plaintext to ciphertext
- **Key -** info used in cipher known only to sender/receiver
- **Encipher (encrypt) -** converting plaintext to ciphertext
- **Decipher (decrypt) -** recovering plaintext from ciphertext
- **Cryptography -** study of encryption principles/methods
- **Cryptanalysis (codebreaking) -** study of principles/ methods of deciphering ciphertext *without* knowing key
- **Cryptology -** field of both cryptography and cryptanalysis

Need of Security

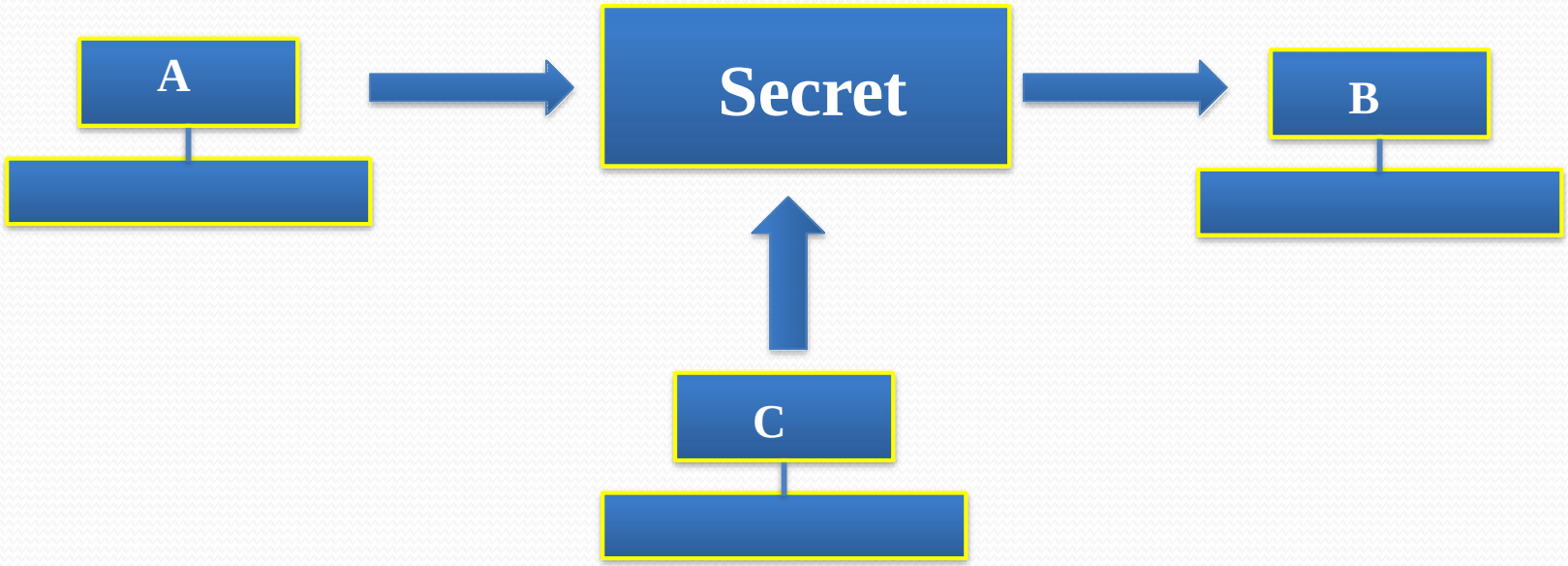


Principle of Security

- Confidentiality
- Integrity
- Authentication
- Non-Repudiation (non-denial)
- Access Control
- Availability

Confidentiality (Interception)

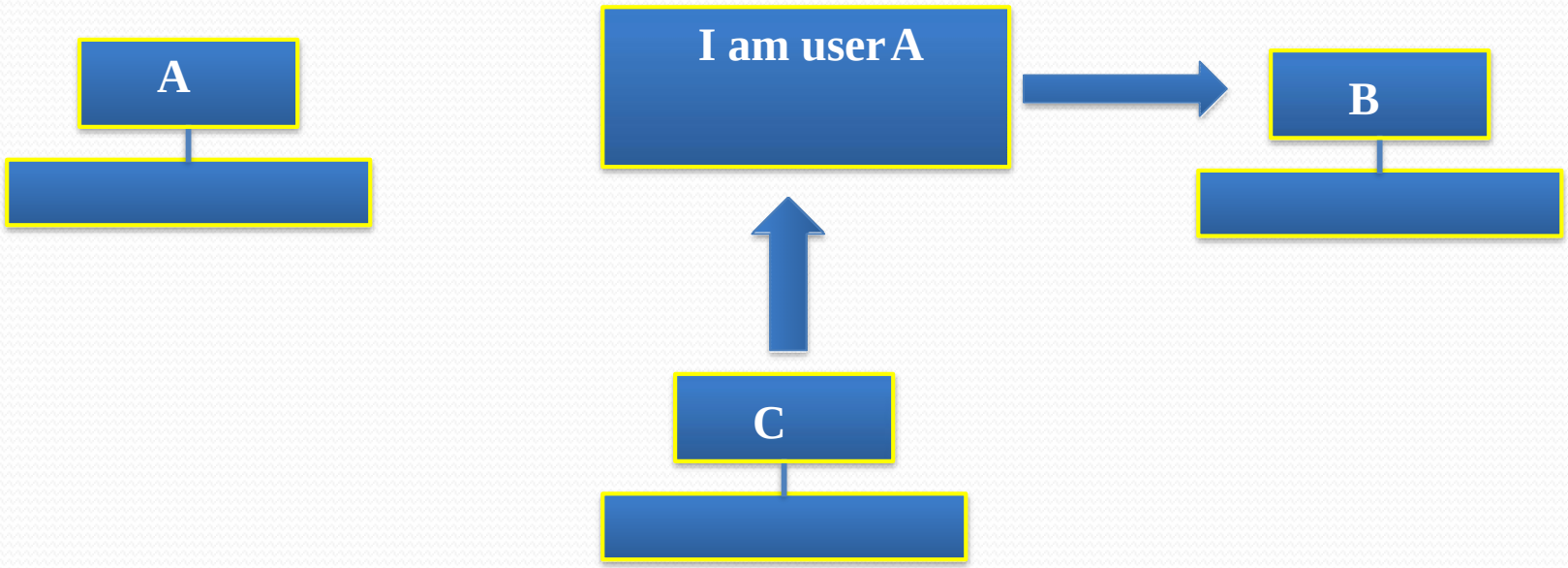
- The principle of Confidentiality specifies that only the sender and the intended recipient(s) should be able to access the contents of a message.



- Another user C gets access to this message, which is not desired and therefore, defeats the purpose of Confidentiality.

Authentication (Fabrication)

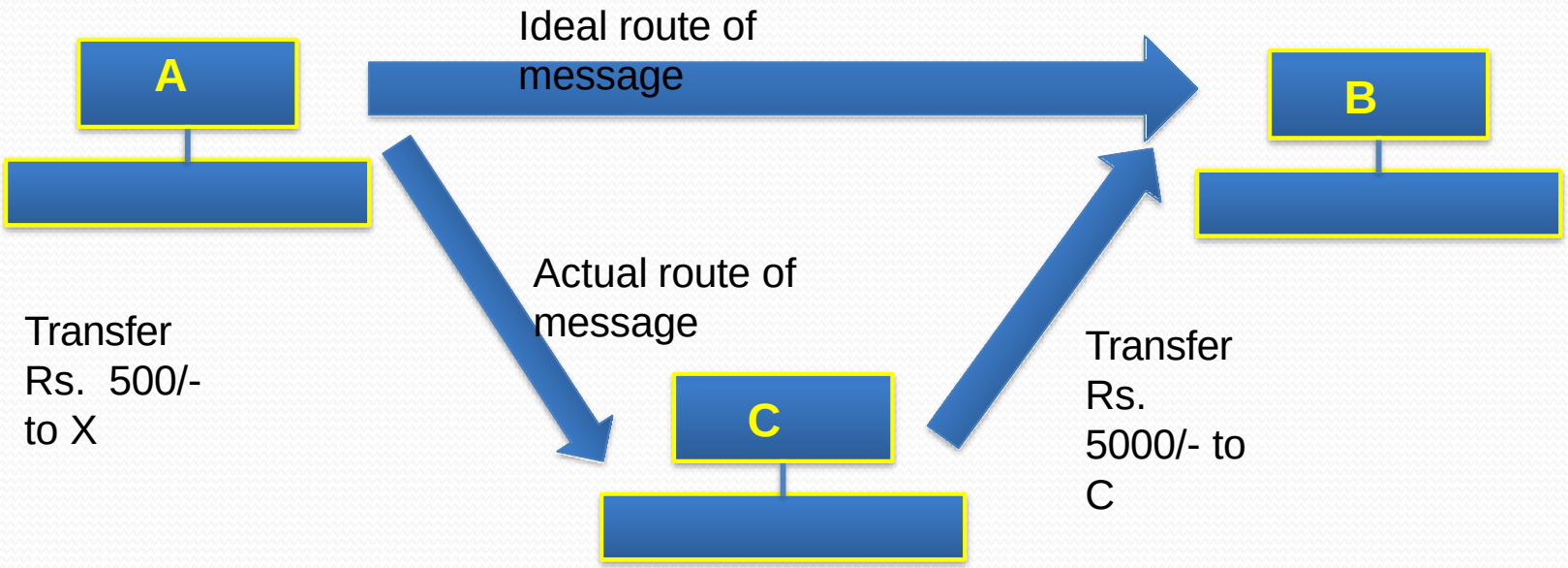
- Authentication mechanisms help establish proof of identities



- User C posting as user A. this type of attack ia called fabrication. Fabrication is possible in absence of proper authentication mechanisms.

Integrity (Modification)

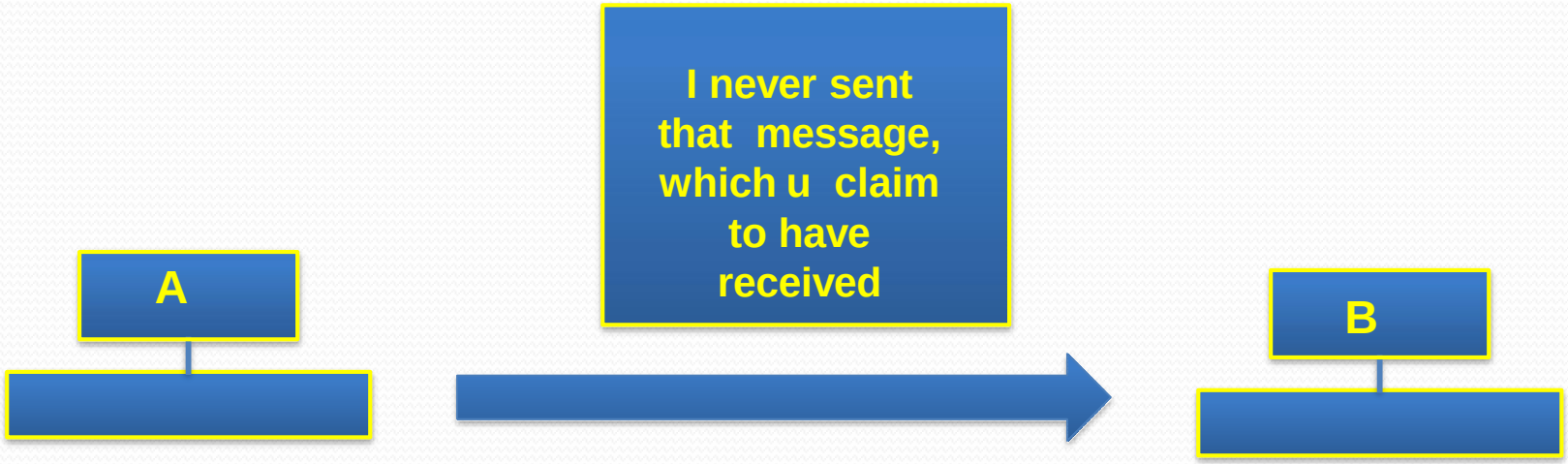
- The contents of a message are changed after the sender sends it, but before it reaches the intended recipient.



- User C manages to access the data, change its contents and send the changed message to user B. this type of attack is called as modification.

Non-Repudiation (non-denial)

- The principle of non-repudiation defeats any possibilities of
  denying something have done.



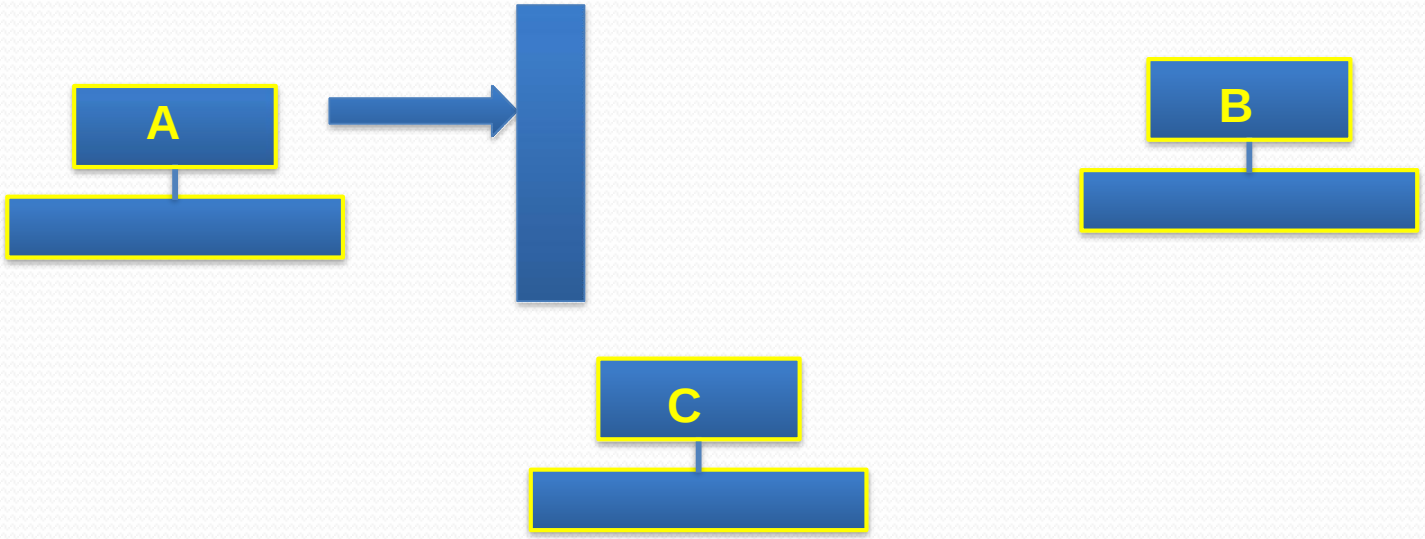
- Non-repudiation does not allow the sender of a message to refuse the claim of not sending that message.

Access Control

- The principle of *access control* determines *who* should be able to access *what.*
- *Access control specifies and controls who can access what.*
- *Eg:* user A can write to file X, but can only update files Y and Z.

Availability (Interruption)

- The principle of availability states that resources should be available to authorized parties at all times.



- Authorized user A may not be able to contact a server/ computer B, due t intentional actions of an unauthorized user C

OSI standard for Security Model

- Authentication
- Access Control
- Non-Repudiation
- Data Integrity
- Confidentiality
- Assurance or Availability

Introduction

- The OSI (open systems interconnection) security architecture provides a systematic framework for defining security attacks, security mechanisms and security services.

Aspects of Security

- consider 3 aspects of information security:
  - **security attack**
  - **security mechanism (control)**
  - **security service**
- note terms
  - *threat* – a potential for violation of security
  - *vulnerability* – a way by which loss can happen
  - *attack* – an assault on system security, a deliberate attempt to evade security 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.

Security Attacks

- A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- *Passive attacks* are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.
- Two types of passive attacks are:

a. Release of message contents:

b. Traffic analysis - monitor traffic flow to determine location and identity of communicating hosts and could observe the frequency and length of messages being exchanged

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

Active Attacks

- The active attacks are based on the modification of the original message in some particular manner or on creation of a false message.
- These attacks cannot be prevented easily.
- However efforts can be taken to detect them and recover from them

These attacks can be in the form of :-

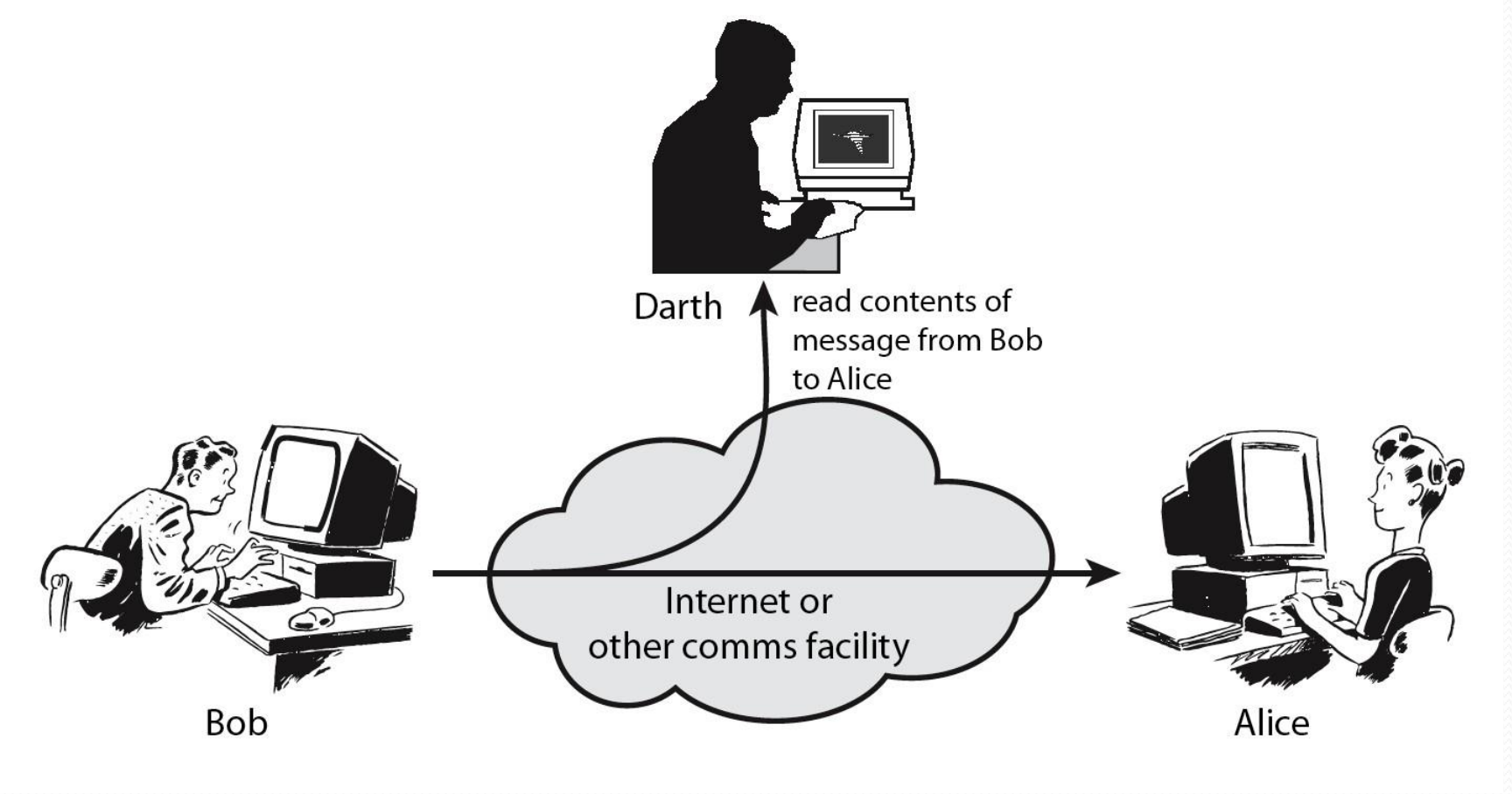
1.) Masquerade.

2.) Replay.

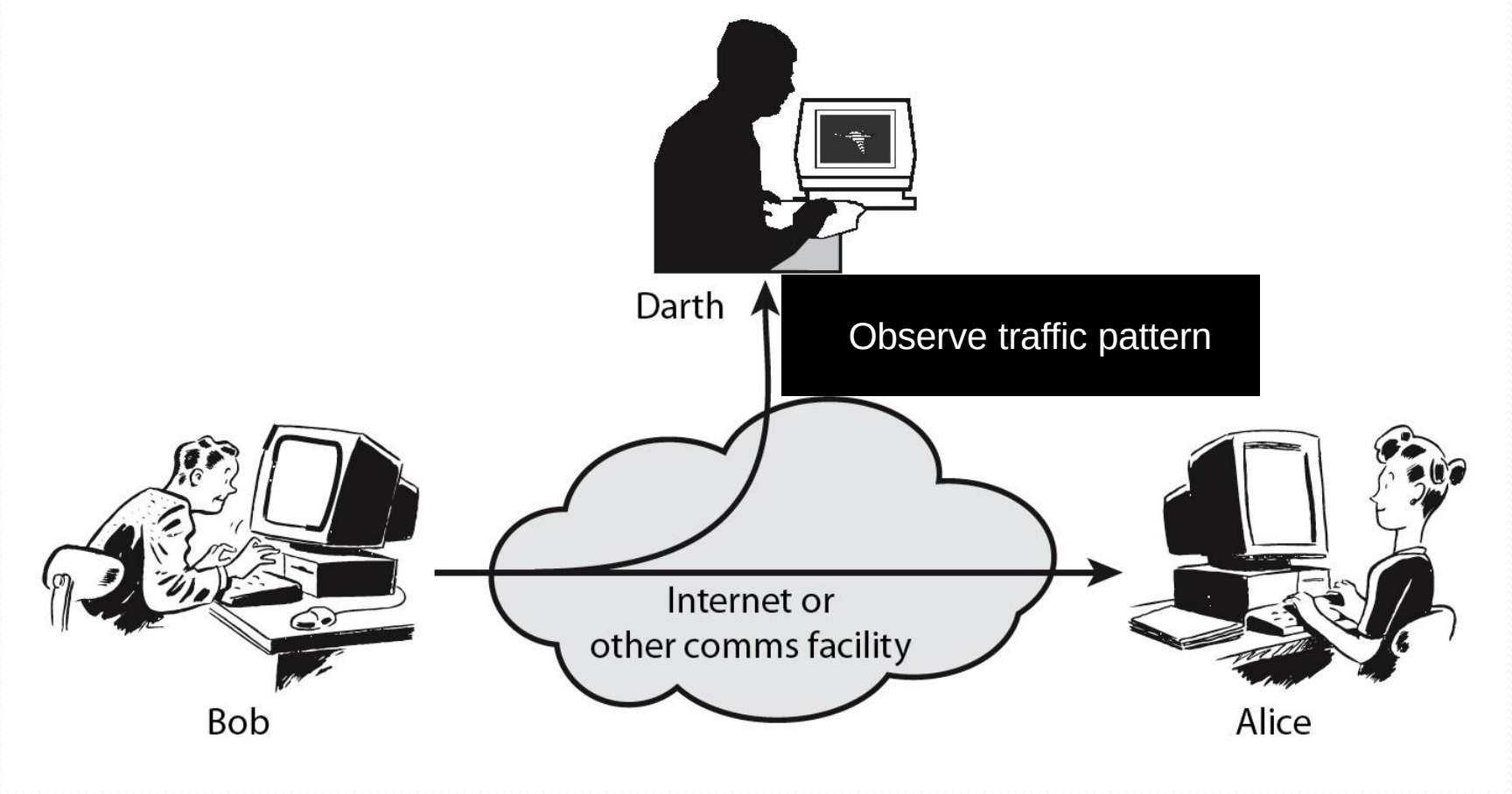
3.) Modification.

4.) Denial of Service

Passive Attack - Interception



Passive Attack: Traffic Analysis



Active Attacks

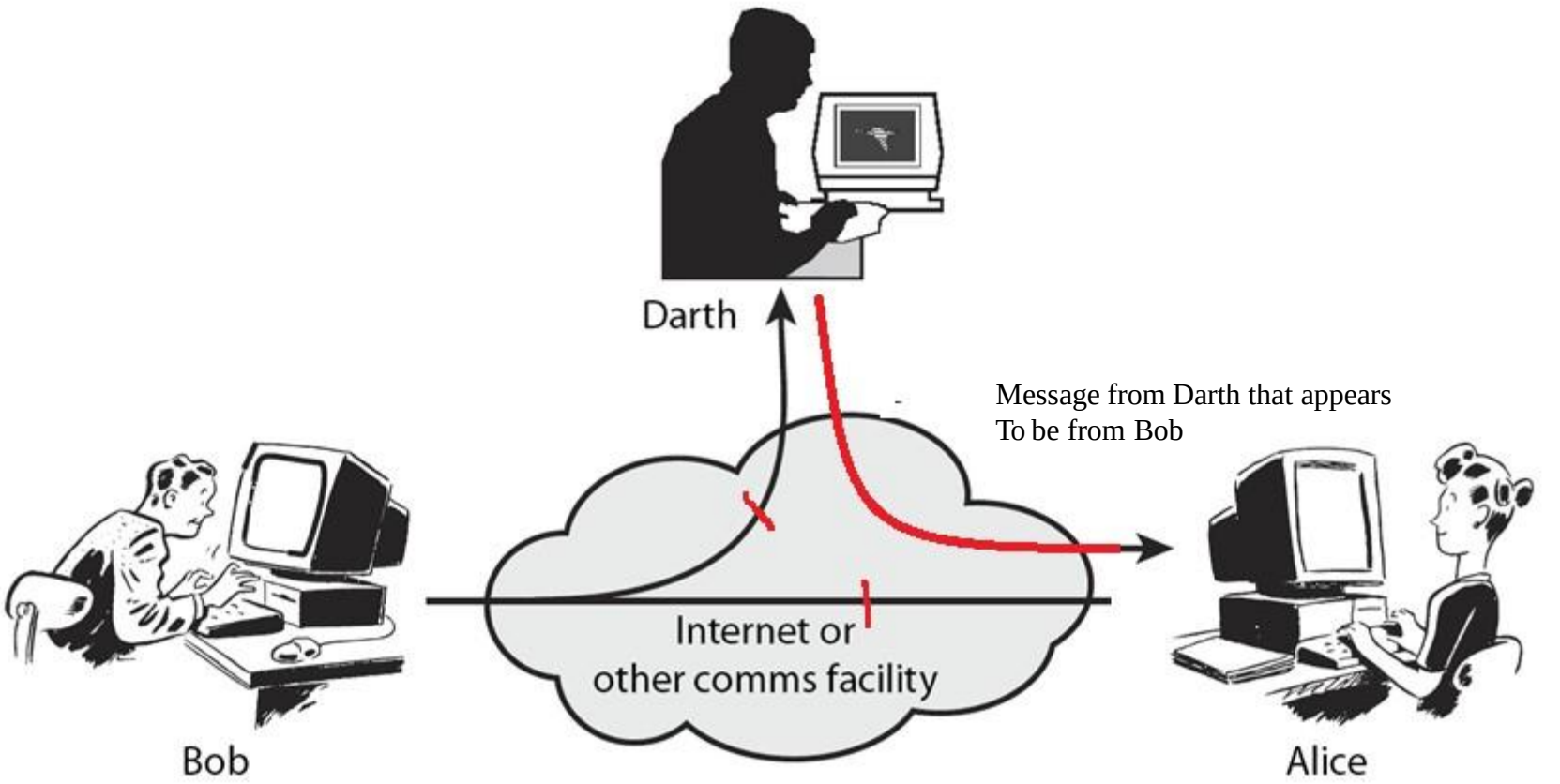
- Active attacks involve some modification of the data stream or the creation of a false stream .
- Subdivided into four categories: masquerade, replay, modification of messages, and denial of service.
- masquerade of one entity as some other.
- replay previous messages.
- modify/alter (part of) messages in transit to produce an unauthorized effect
- denial of service - prevents or inhibits the normal use or management of communications facilities

A **masquerade attack** is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.

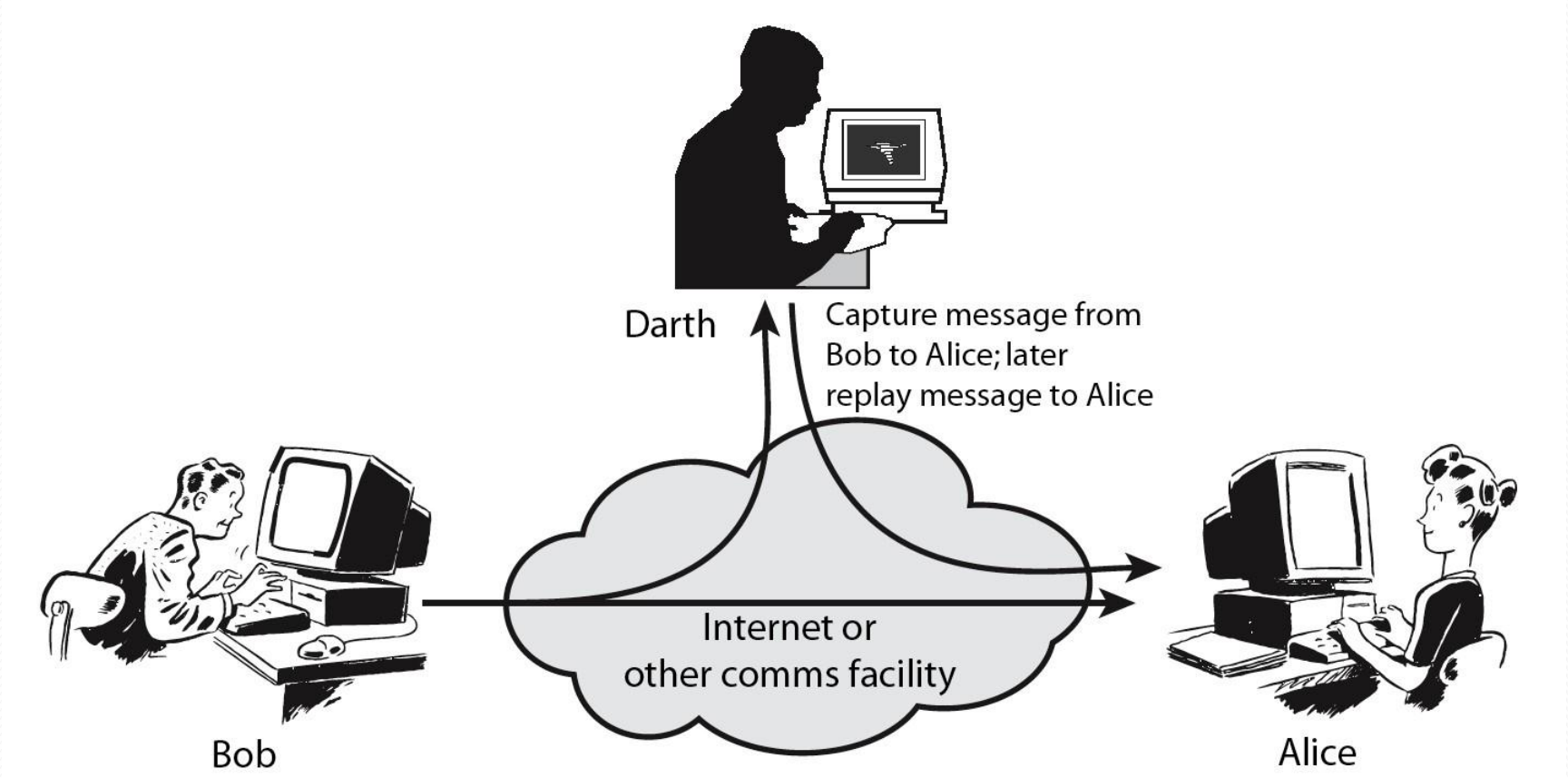
Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process.

A **replay attack** (also known as **playback attack**) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it
Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides ; meanwhile, Eve is eavesdropping on the conversation and keeps the password. After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts thus granting access to Eve.

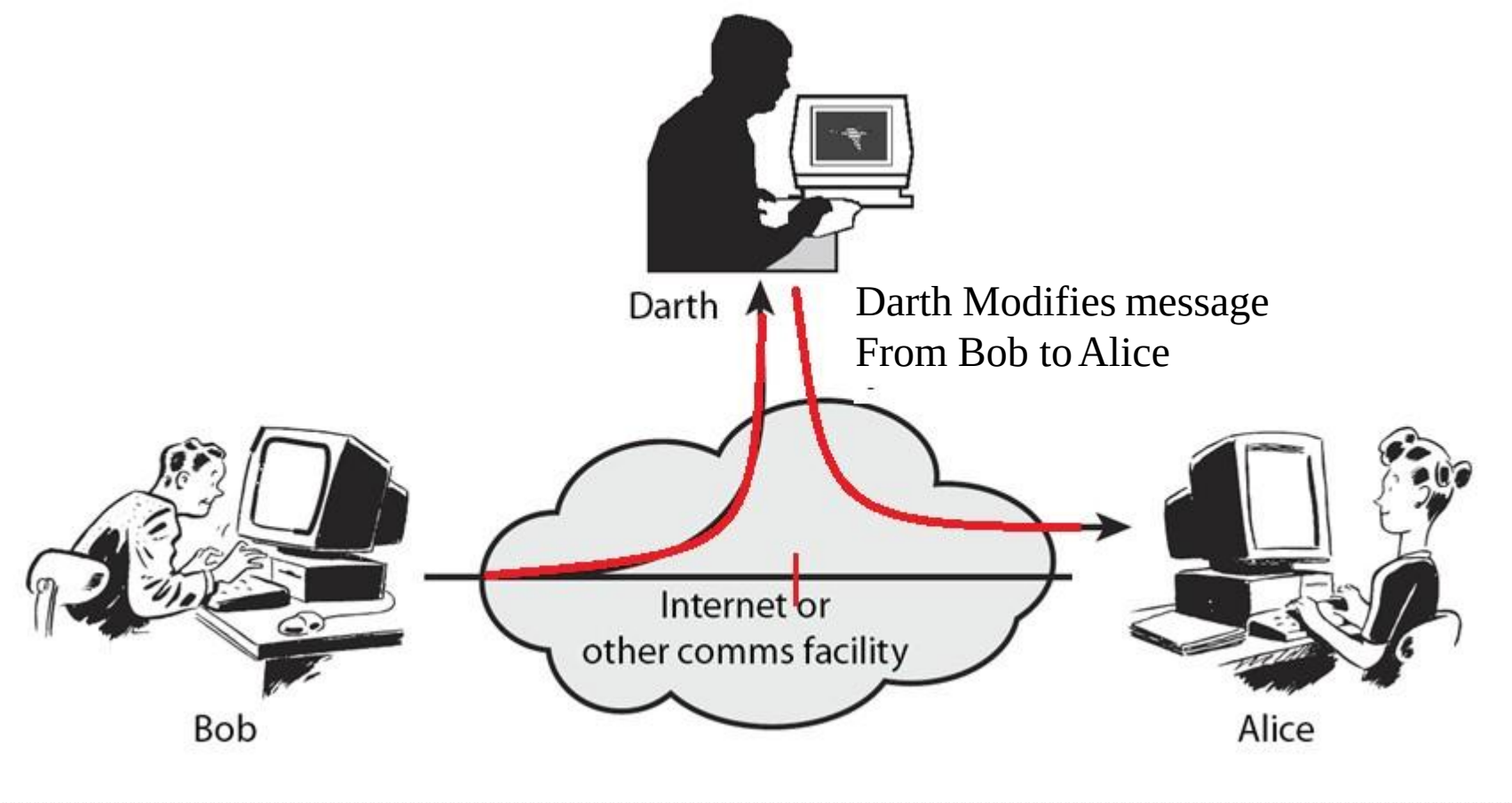
Active Attack: Masquerade



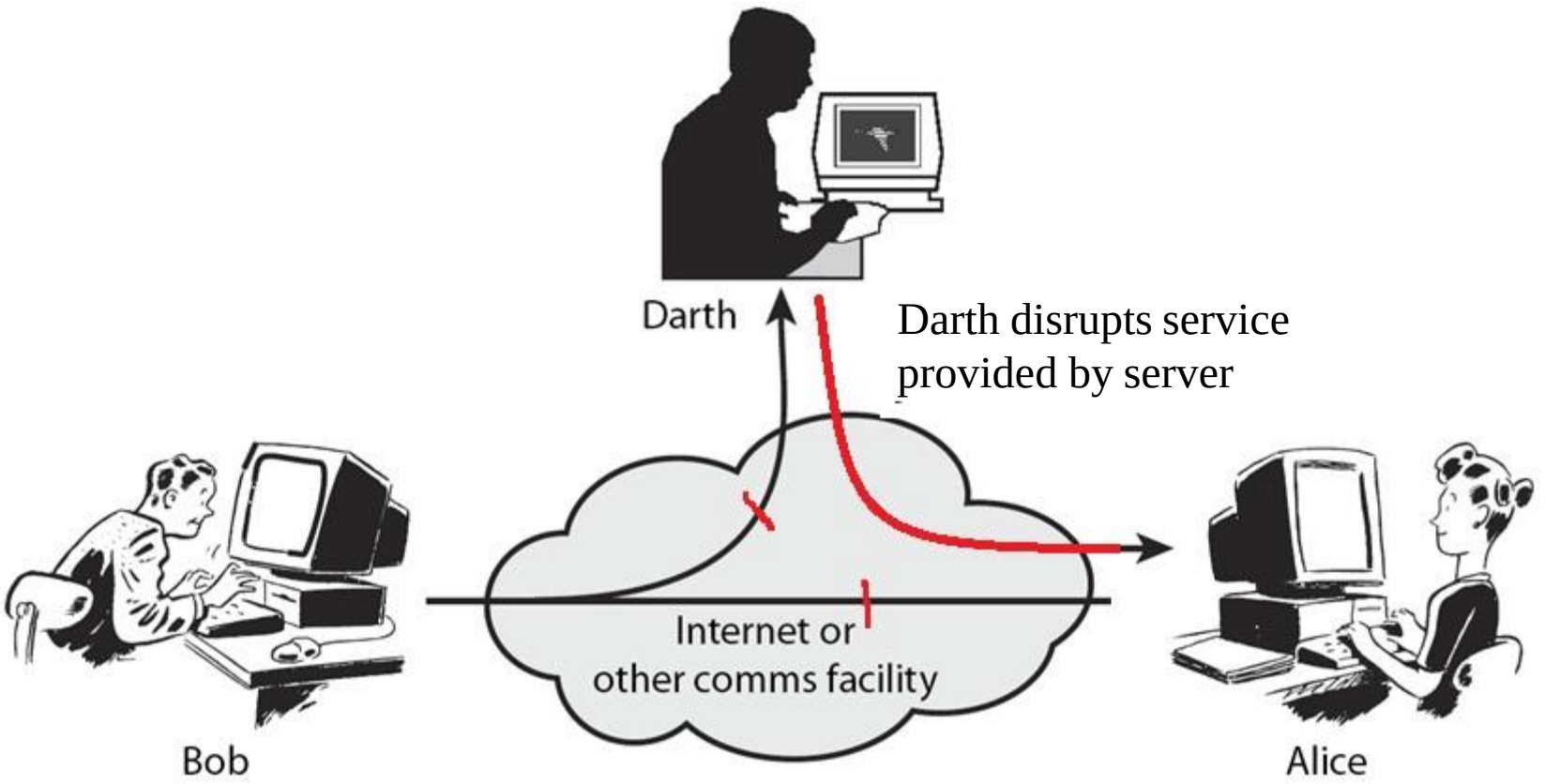
Active Attack: Replay



Active Attack: Modification



Active Attack: Denial of service



Handling Attacks

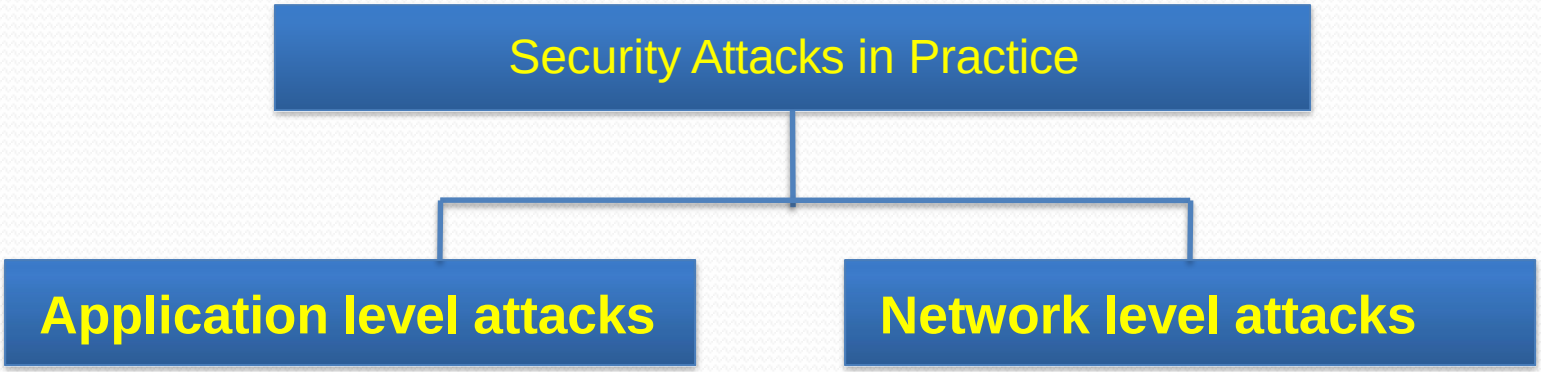
- Passive attacks – focus on Prevention
  - Easy to stop
  - Hard to detect
- Active attacks – focus on Detection and Recovery
  - Hard to stop
  - Easy to detect

Classification of attacks

- Attacks can be classified into two broad categories:

A. Application-level attacks

B. Network-level attacks



- **Application level attacks-** the attacker attempts to access, modify or prevent access to information of a particular application or to the application itself.
- Eg: obtain credit card information on internet or changing the content of message.
- **Network level attacks-** Aim at reducing the capabilities of a network by a number of possible means. These attacks generally make an attempt to either slow down or completely bring to halt, a computer network.

Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- 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