SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

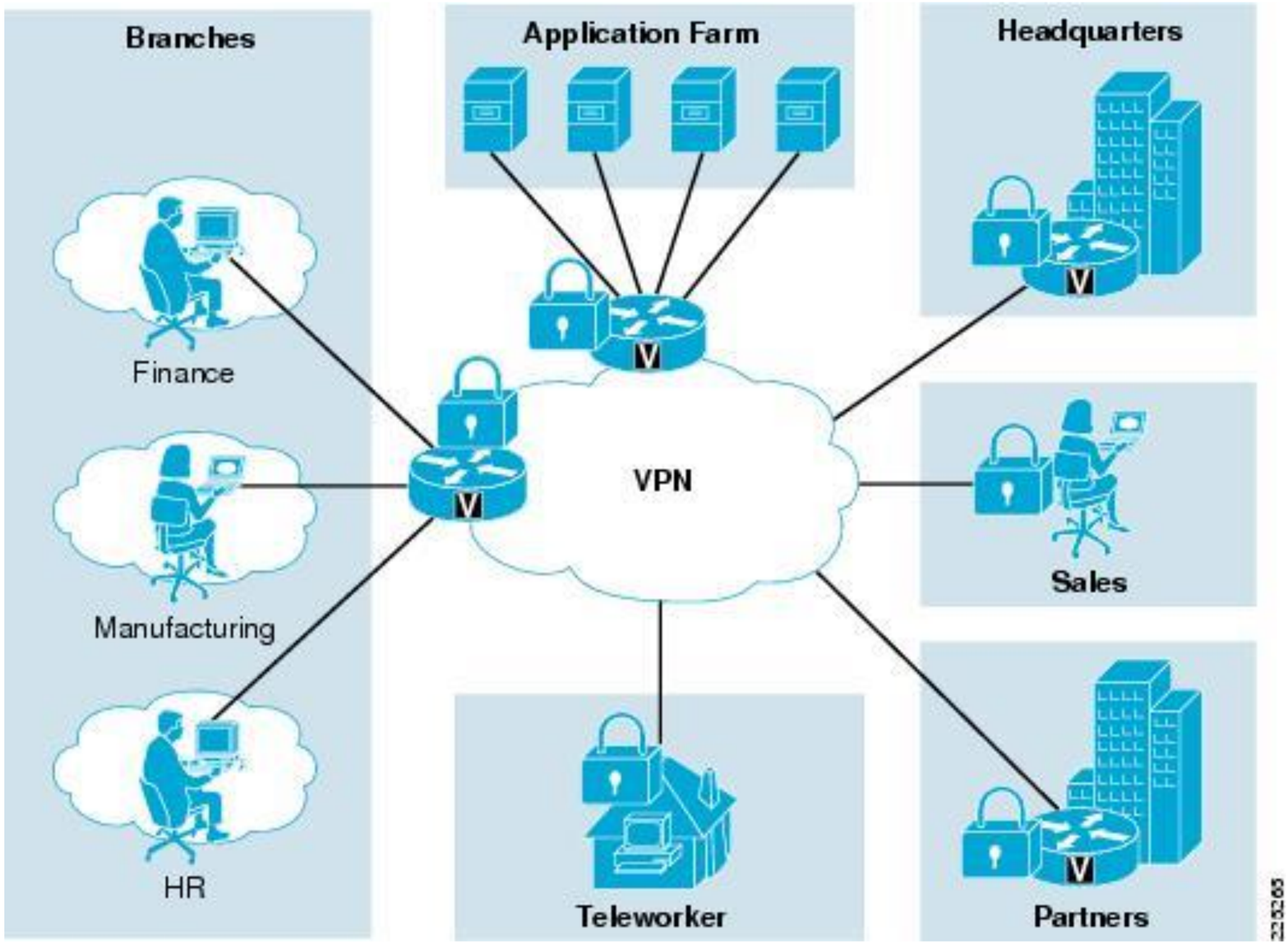
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME : 19CS503-Cryptography and Network Security

III YEAR /V SEMESTER

Unit 1- Introduction

Topic : Security attacks, services and mechanisms – OSI security architecture


Branches
Application Farm
Headquarters
Finance
Manufacturing
HR
VPN
Sales
Teleworker
Partners
223263

Terms Used

Information Security

physical or Administrative

unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction

Terms Used

Network Security

business, government and academic organization

Interconnect their data processing equipment with a collection of interconnected networks

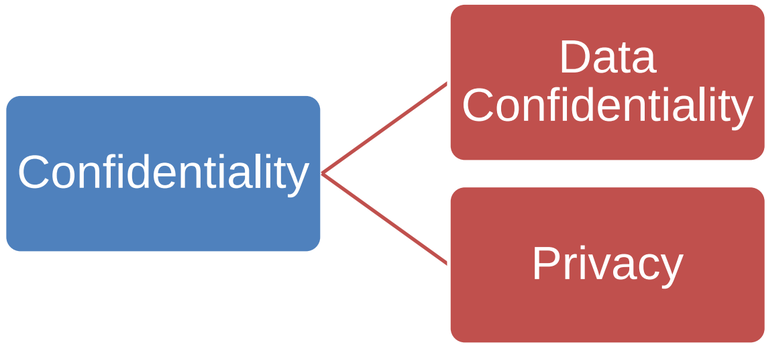
Terms Used

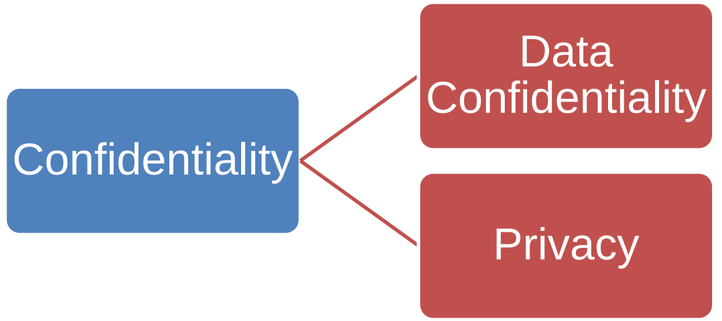
Computer Security

telephone network, data network or over internet

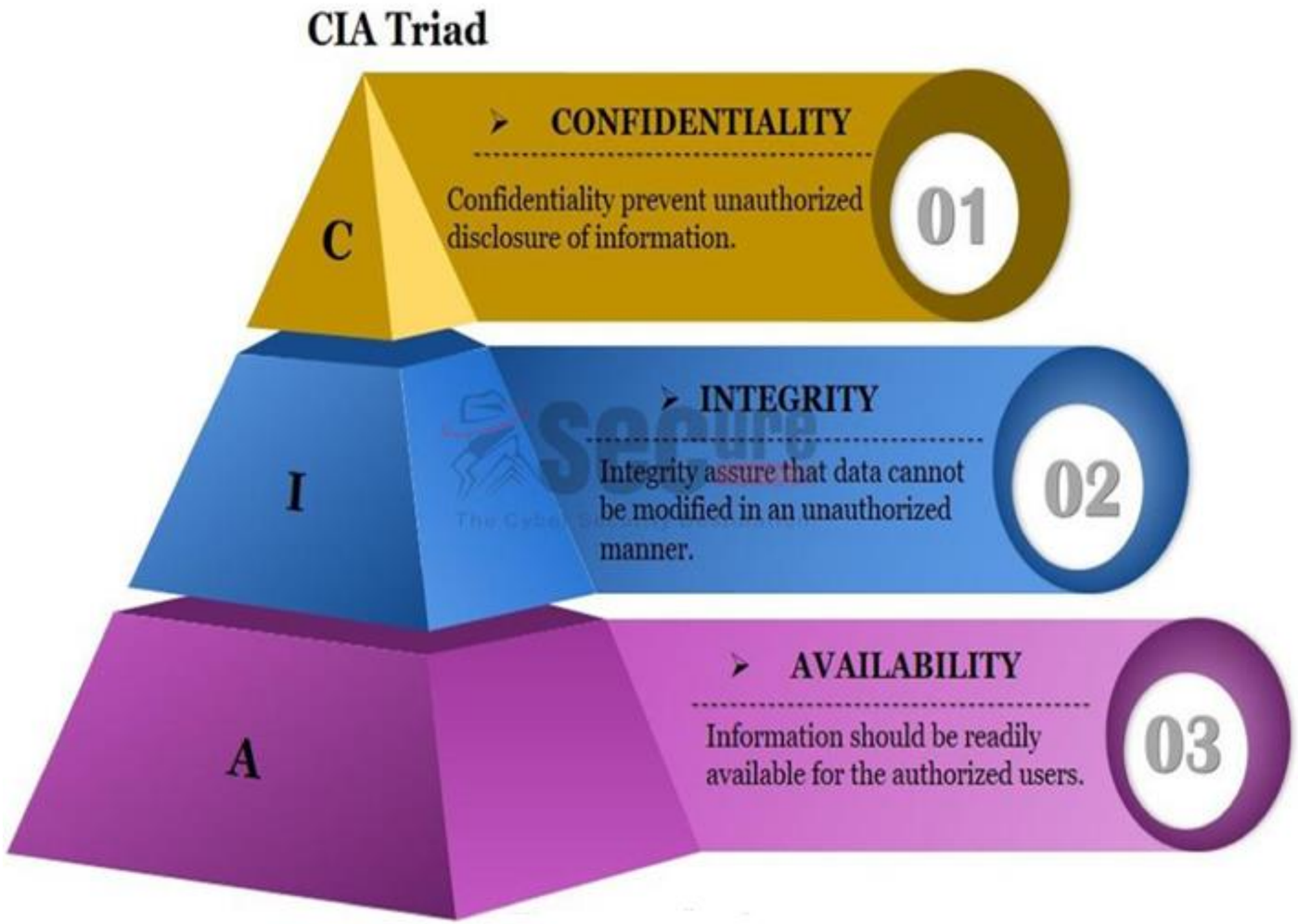
Protect data and thwart hackers

Key Security Concepts





CIA Triad

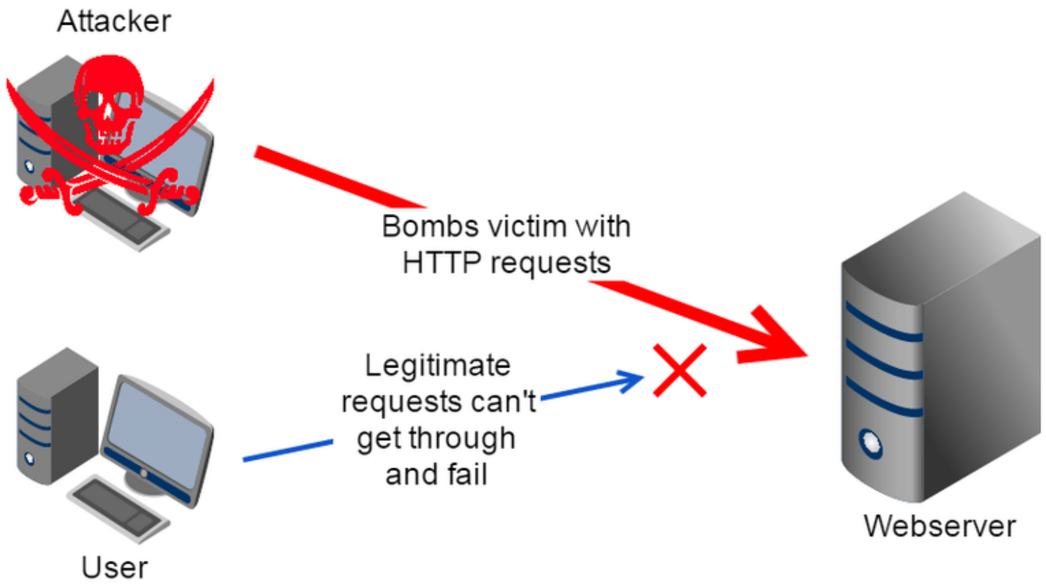

CIA Triad
C
CONFIDENTIALITY
Confidentiality prevent unauthorized disclosure of information.
01
I
INTEGRITY
Integrity assure that data cannot be modified in an unauthorized manner.
02
A
AVAILABILITY
Information should be readily available for the authorized users.
03

Security Attacks

- **Active Attack** – Modification of data stream or creation of false stream.
- **Passive Attack** – N/w Attack. Gain information about the target and no data is changed on the target.
  - Release the Message content
  - Traffic Analysis

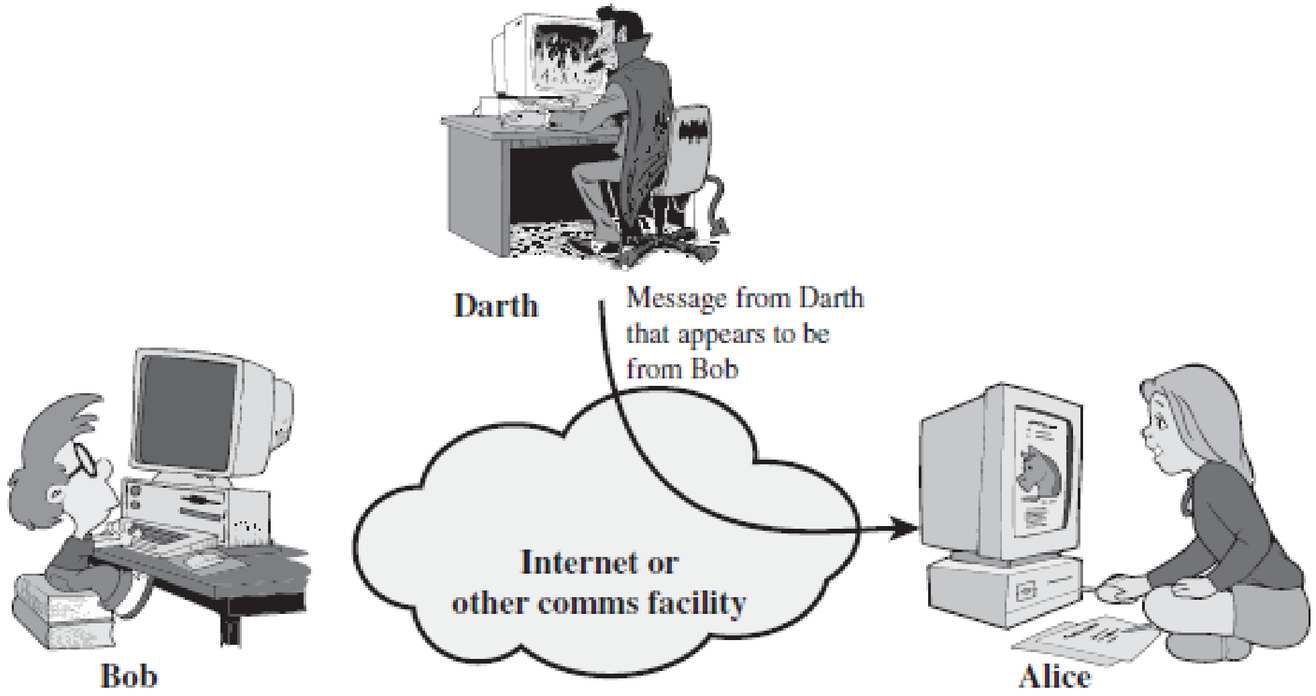
Activity

Types of Active Attack



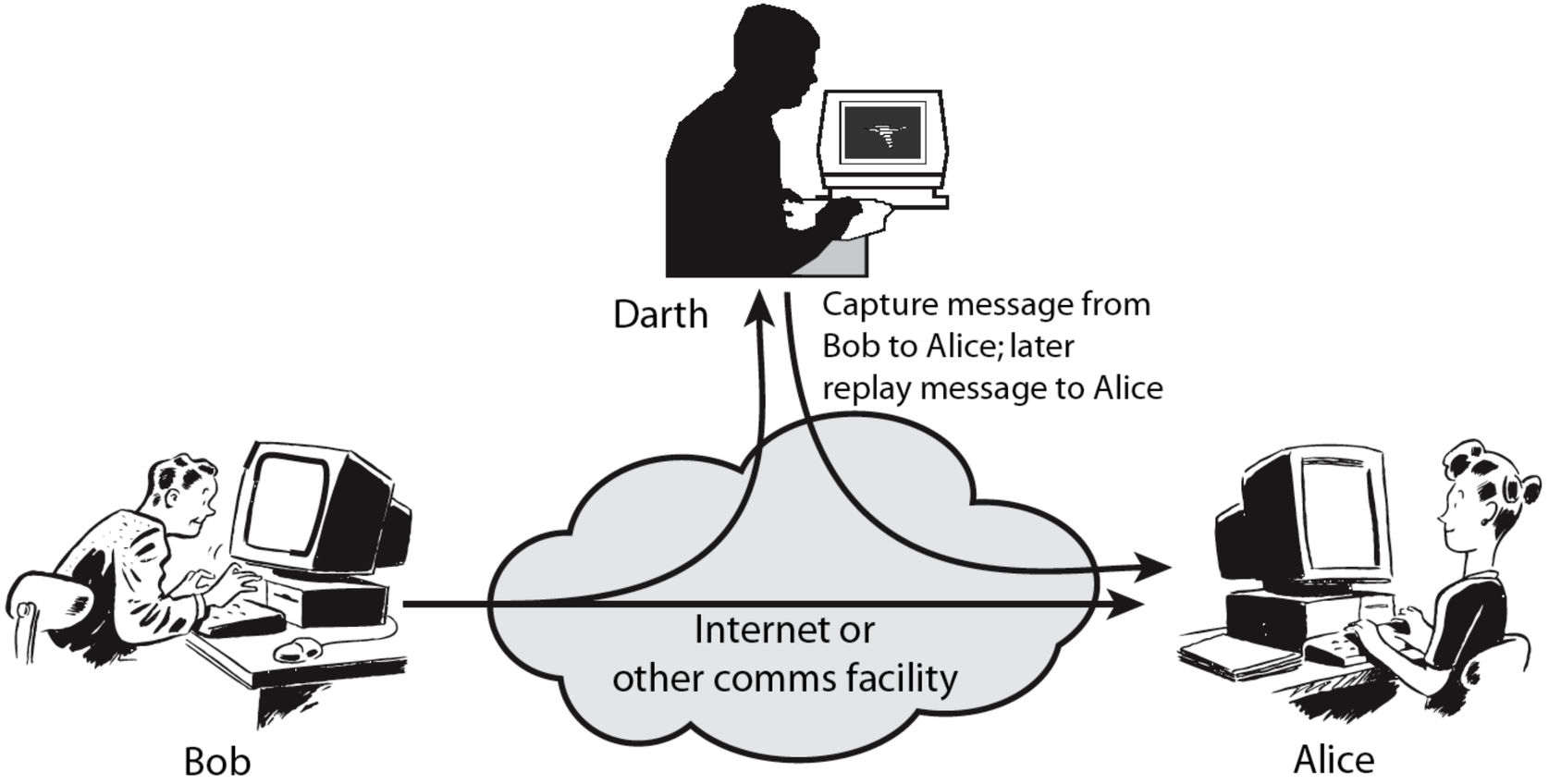
–Masquerade
–Replay
–Modification
–Denial of Services

Active Attacks -Masquerade

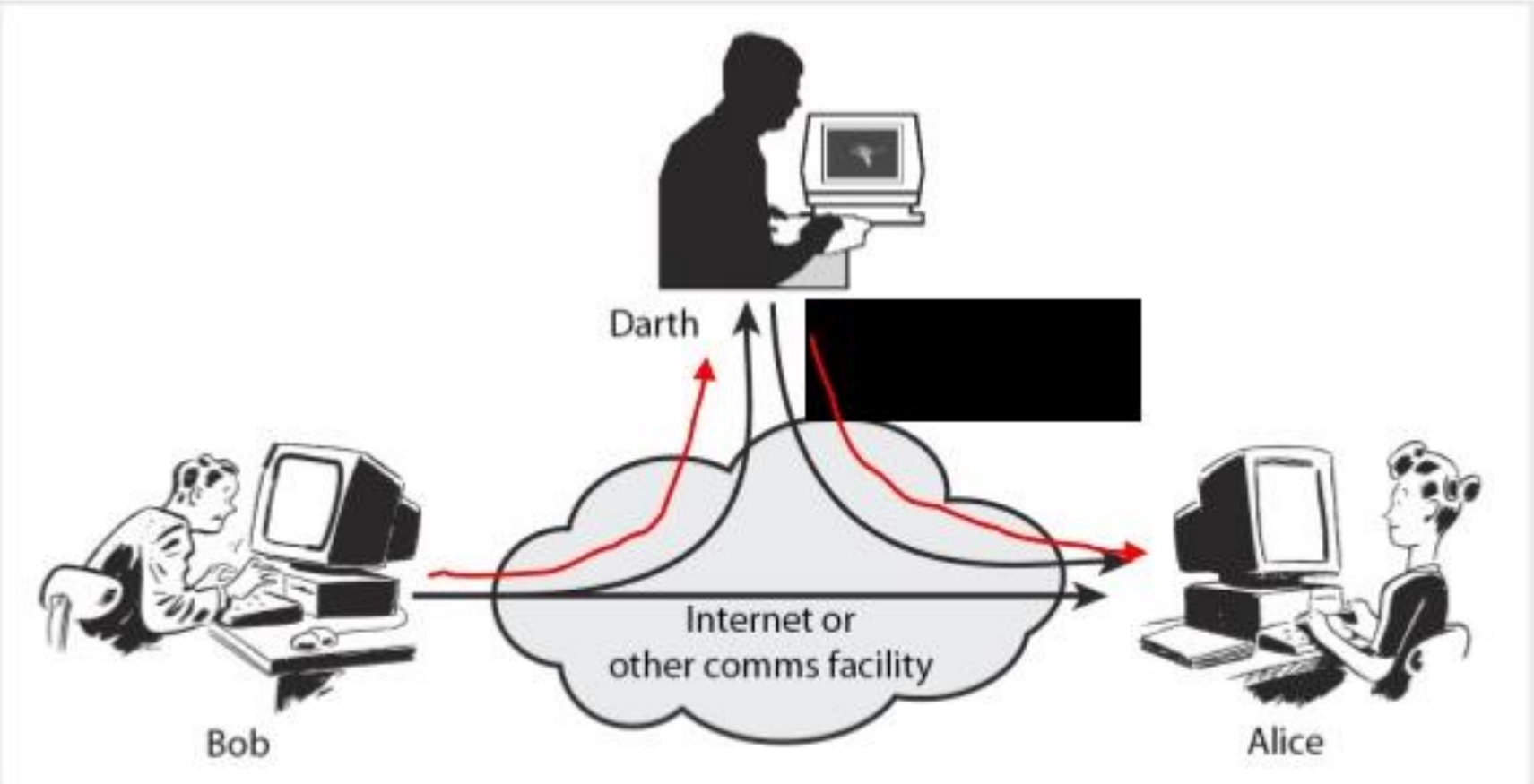


(a) Masquerade

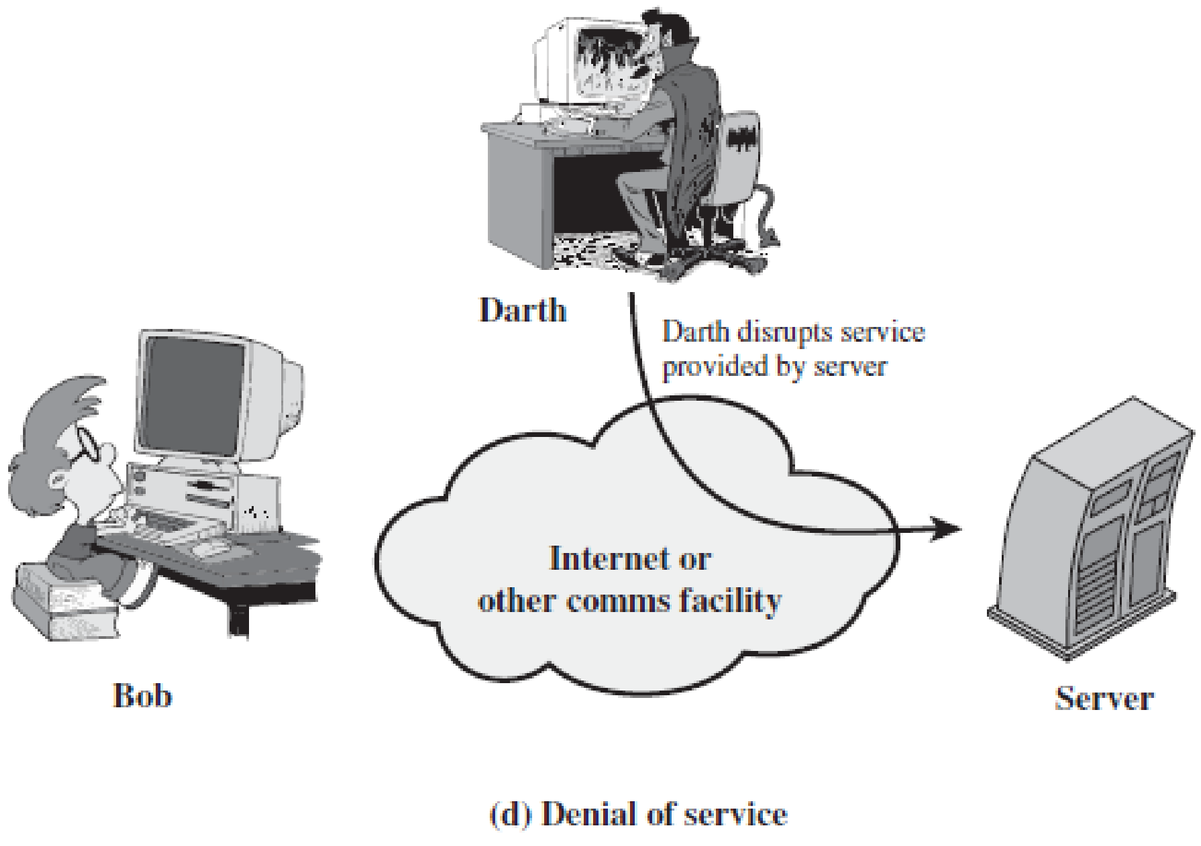
Active Attacks -Replay



Active Attacks - Modification

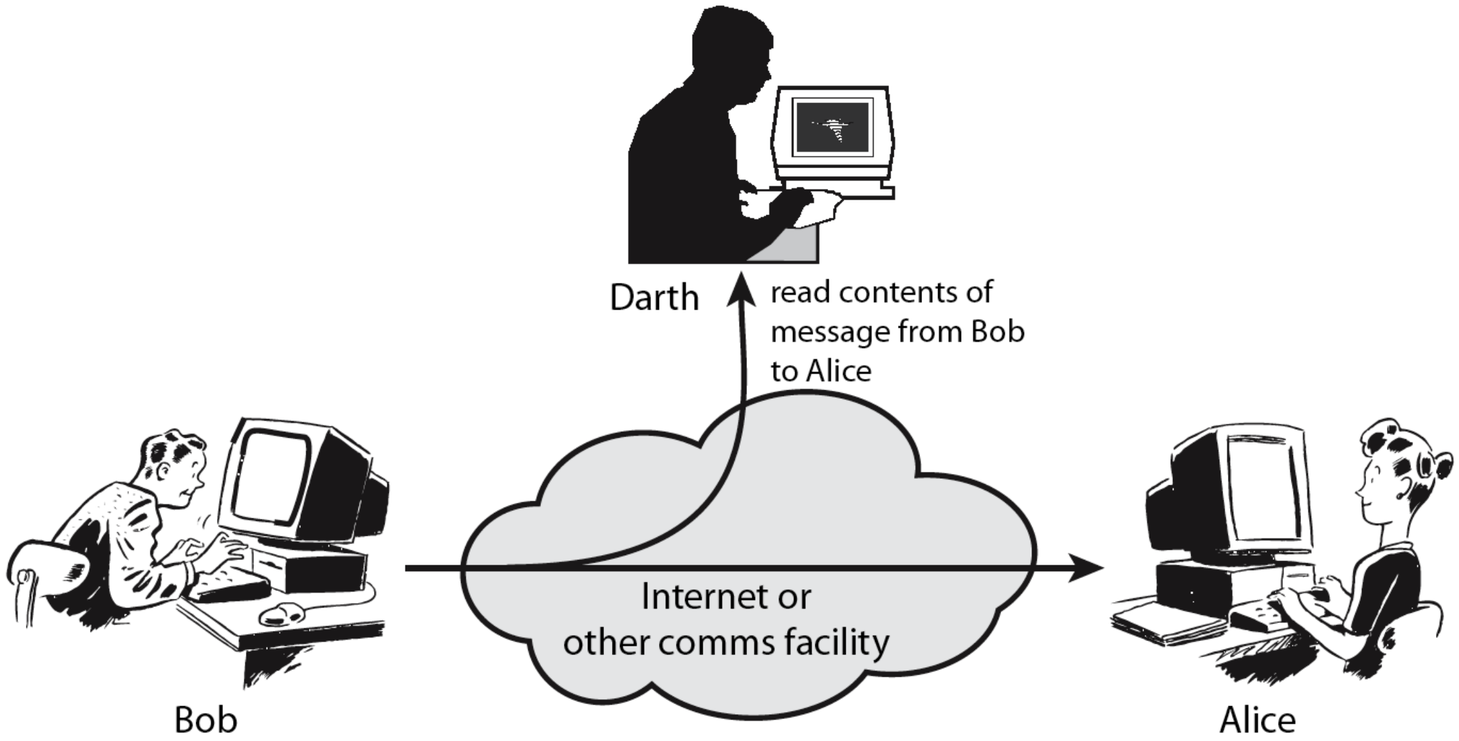


Active Attacks - DOS

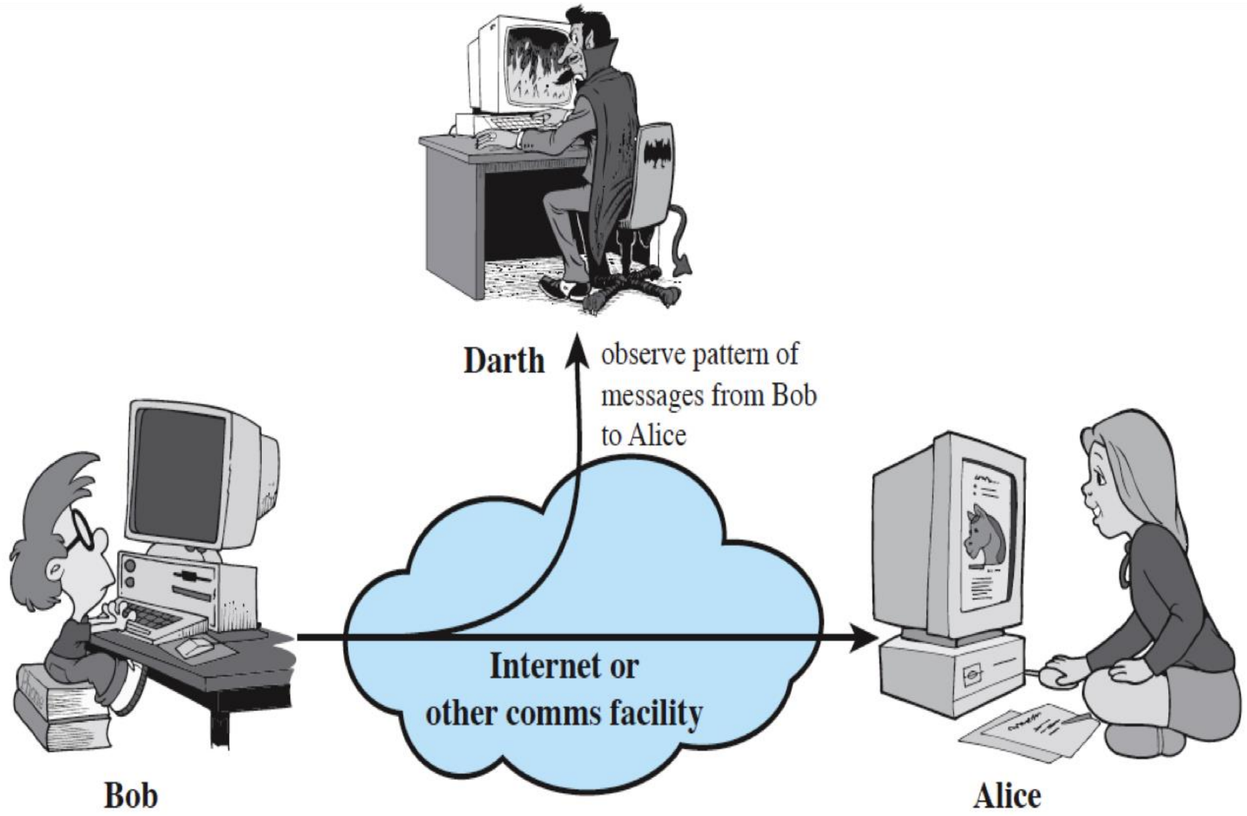


(d) Denial of service

Passive Attack - Release the Message content



Passive Attack – Traffic Analysis



Security Services

- **Authentication** - assurance that communicating entity is the one claimed
  - **–Peer-entity Authentication - Logical connection**
  - **–Data origin authentication – Connectionless Transfer**
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
  - **–Connection Confidentiality**
  - **–Connectionless Confidentiality**
  - **–Selective Field Confidentiality**
  - **–Traffic Flow Confidentiality**

Security Services

Data Integrity - Assurance that data received is as sent by an authorized entity

- Connection Integrity with Recovery
- Connection Integrity without Recovery
- Selective Field Connection Integrity
- Connectionless Integrity
- Selective Field Connectionless Integrity

Non-Repudiation - Protection against denial by one of the parties in a communication

- Non-Repudiation, Origin
- Non-Repudiation Destination

Security Mechanisms

Specific security mechanisms

- **Encipherment** – use mathematical algorithm to transform data
- **Digital Signatures** – data Appended to cryptographic
- **Access Controls** – Access rights to resources
- **Data Integrity** – Assure the data
- **Authentication Exchange** – Ensure the Identity
- **Traffic Padding** – Insert bits into gaps
- **Routing Control** – Secure routes
- **Notarization** – use third party to assure the data

Security Mechanisms

Pervasive Security Mechanisms:

- **Trusted Functionality**
- **Security Labels**
- **Event Detection**
- **Security Audit Trails**
- **Security Recovery**

Assessment 1

1. Network Security provides authentication and access control for resources.
   a) True
   b) False

2 The process of verifying the identity of a user.
   a) Authentication
   b) Identification
   c) Validation
   d) Verification

REFERENCES

1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2013.

THANK YOU