Course Name- Computer, Data and Network Security

Course Instructor:

Dr. Md. Shariful Islam

Professor, IIT, DU

shariful@iit.du.ac.bd

Suggested Readings

Text Book:

1.Cryptography and Network Security : Principles and Practice (5th edition) by William Stallings

2. Computer Security : Principles and Practice by William Stallings and L. Browne

Research Papers:

Research Papers on related topics will be provided for seminar presentation.

Course Administration

Mid Terms (20 Marks) [Avg]:

- Prescheduled Mid# 1 – 20 marks
- Prescheduled (if possible) Mid#2 – 20 marks
- Only average marks will be counted

Assignments (20 Marks)

Class Attendance (10 Marks)

Final Examination (50 Marks)

Lab (50 Marks)

AGENDA

- Overview of Network security
- Security Goals
- Security Mechanisms
- Security Services

NETWORK SECURITY

field of network security

- how bad guys can attack computer networks?
- how we can defend networks against attacks?
- how to design architectures that are immune to attacks?

Internet not originally designed with (much) security in mind

- *original vision:* "a group of mutually trusting users attached to a transparent network"
- Internet protocol designers playing "catch-up"
- security considerations in all layers!

INFORMATION SECURITY DEALS WITH

Security of end systems

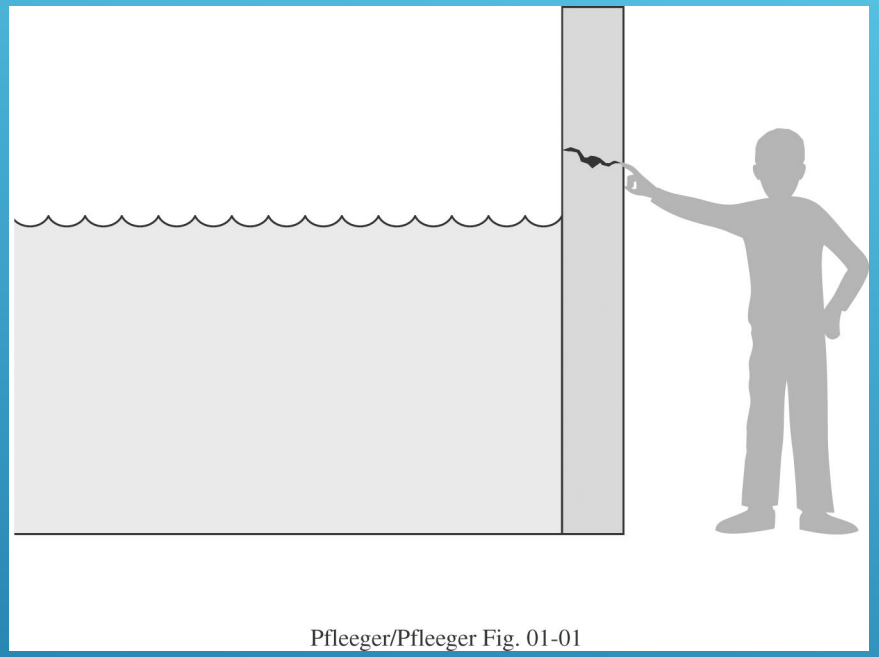
- Examples: Operating system, files in a host, databases, accounting information, logs, etc.

Security of information in transit over a network

- Examples: e-commerce transactions, online banking, confidential e-mails, file transfers, etc.

SOME TERMINOLOGIES

Threat	Set of circumstances that has the potential to cause loss or harm
Vulnerability	a weakness in the security system (in procedures, design and implementation)
Control	Some protective measures



Pfleeger/Pfleeger Fig. 01-01

A *THREAT* IS BLOCKED BY *CONTROL* OF *VULNERABILITIES*

TYPES OF THREATS

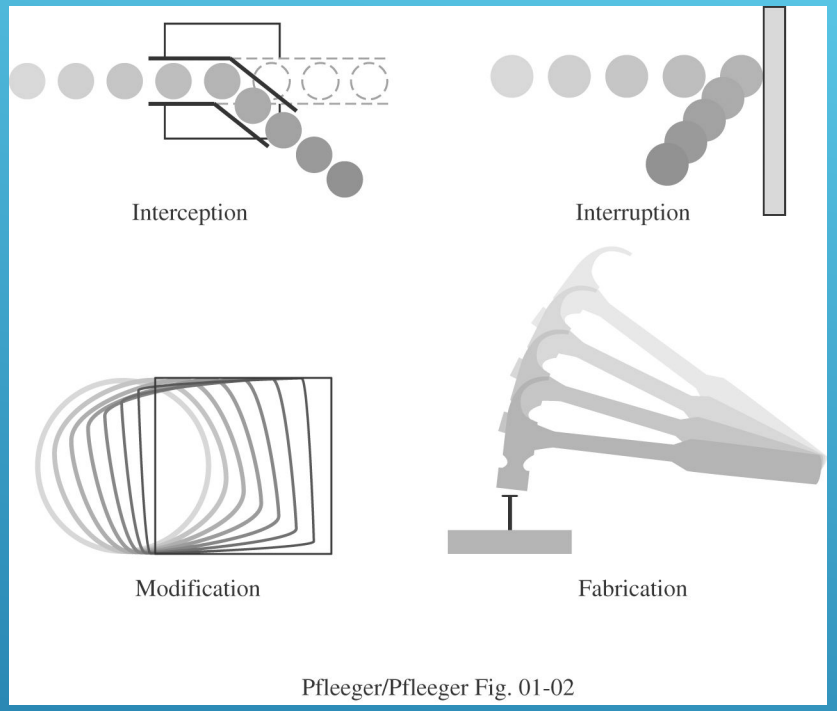
Interception

- Un-authorized party gained access to an asset.
- Illegal copying of program or data.
- Example: Wiretapping to obtain data in a network.

Interruption

- an asset of the system become lost, unavailable or unusable.
- Hardware failure
- Operating system malfunction
- Example Erasure of a program or data file

TYPES OF THREATS (CONT.)



Pfleeger/Pfleeger Fig. 01-02

TYPES OF THREATS (CONT.)

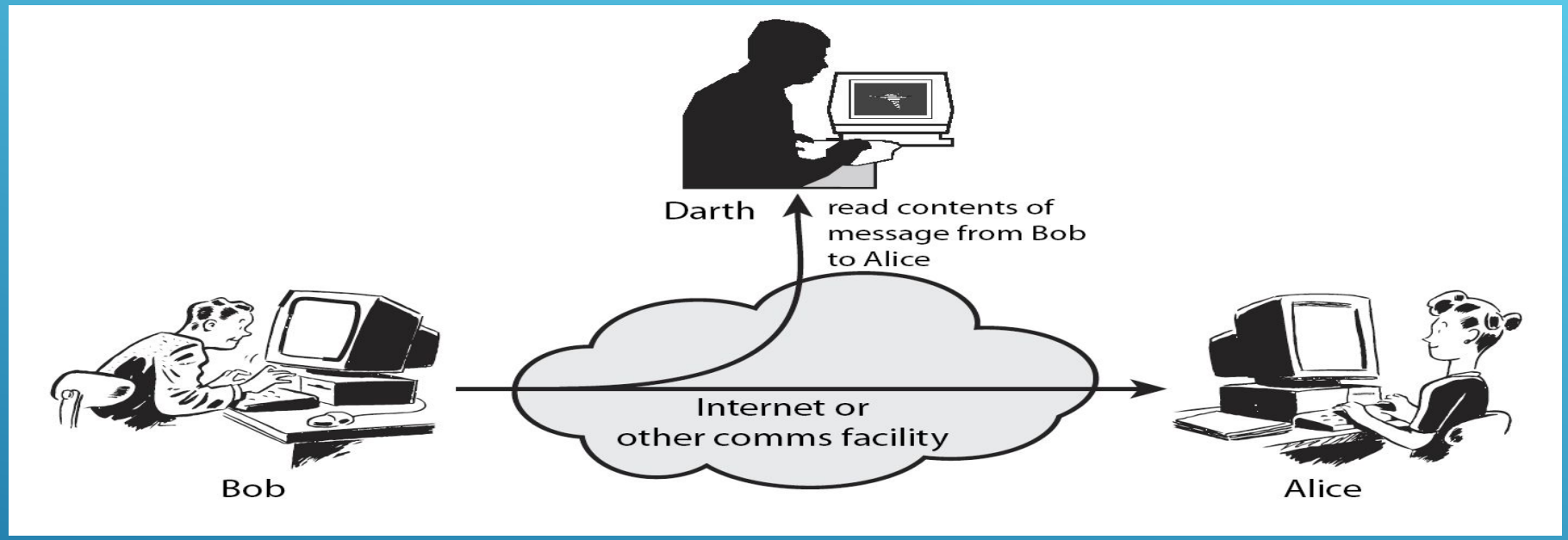
Modification

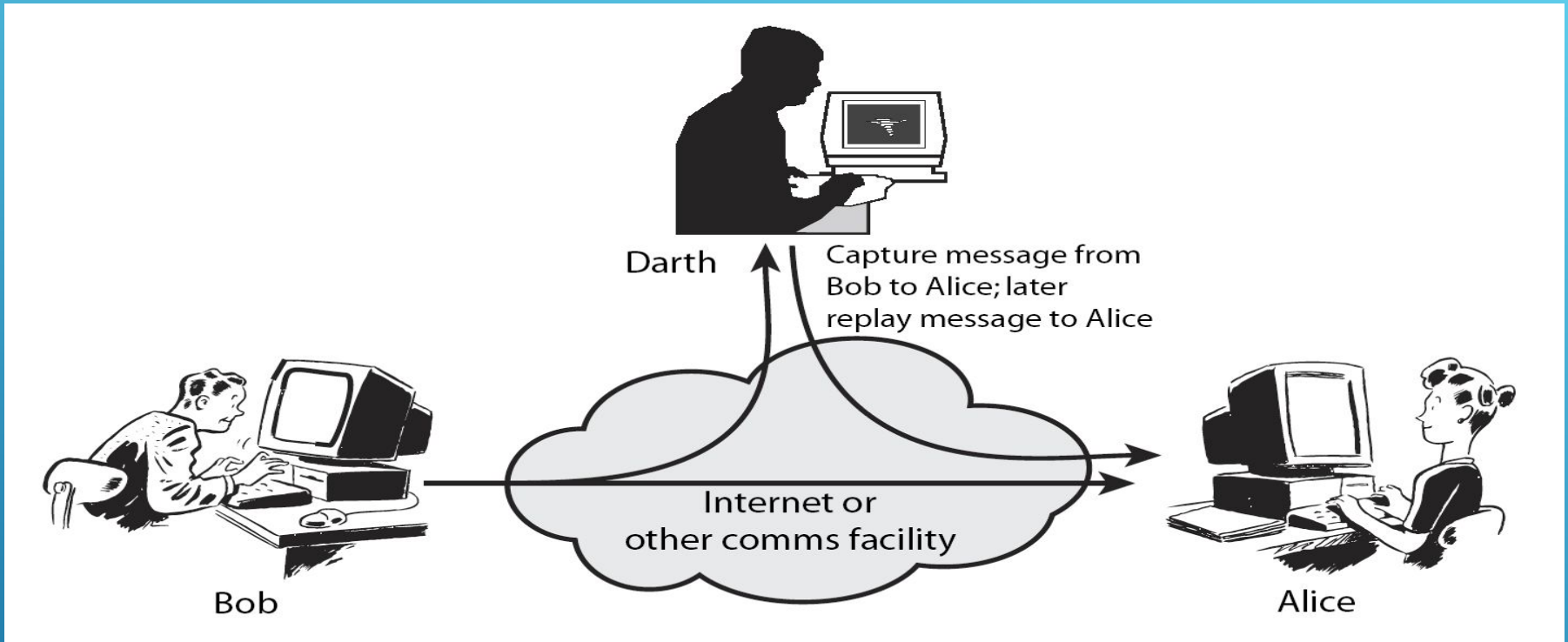
- Not only an-authorized access, but tampers with an asset.
- Example: Alteration of data

Fabrication

- Addition of imaginary information to a system by an un authorized party.
- Example: addition of a record to an existing database

PASSIVE ATTACK





ACTIVE ATTACKS

SECURITY GOALS (CIA)

Confidentiality

- Keeping data and resources secret or hidden.(secrecy or privacy)
- Only authorized party can access information.
- access does not mean write but allows to read, view or print information.

Integrity

- Assets can be modified only by authorized parties or only in authorized ways.
- Modification writing, deleting, creating, changing etc.

Availability

- Ensuring authorized access to data and resources when desired

SECURITY SERVICES AND MECHANISMS

Services

- enhances the security of the data processing systems and the information transfers of an organization.
- intended to counter security attacks
- make use of one or more security mechanisms to provide the service.

Mechanisms

- A mechanism that is designed to detect, prevent, or recover from a security attack

SECURITY SERVICES

Authentication	• assurance that communicating entity is the one claimed • have both peer-entity & data origin authentication
Access Control	• prevention of the unauthorized use of a resource
Data Confidentiality	• protection of data from unauthorized disclosure

SECURITY SERVICES

Data Integrity	• assurance that data received is as sent by an authorized entity
Non-Repudiation	• protection against denial by one of the parties in a communication
Availability	• resource accessible/usable

SECURITY MECHANISMS

Enchipherment

- The use of mathematical algorithms to transform data into a form that is not readily intelligible.
- Symmetric and public key encryption mechanisms.
- DES, 3DES, AES, RSA, etc

Digital Signature

- Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).
- Digital Signature Standard (DSS) or RSA based algorithms.

Access Control

- A variety of mechanisms that enforce access rights to resources.
- Discretionary Access Control (DAC) , Role Based Access Control (RBAC) etc.

Data Integrity

- A variety of mechanisms used to assure the integrity of a data unit or stream of data units
- MD5. SHA etc.

CONCLUSION

Discussed about

- Information security
- Security requirements and threats
- Security services and mechanisms
- Malicious programs