Week1. Introduction to Information Security. Basic Terminology.

Lecturer: Igibek Koishybayev
Prepared by: Zhanbolat Seitkulov

Teaching

- Lectures – by Me (15 lectures on a weekly basis)
- Labs and Practical sessions – also by Me

- Contact

  Email: Igibek@mail.usf.edu

  Office 802.

Some information to help you to take this module

Course Objectives

- 15 lectures – one per week
  - Provide overview of Security Principles
    - Encryption, Network Security, Software Security, Data and Network Protection methods
- Laboratory works and Quizzes
- Prerequisites:
  - Information systems
  - Networking
    - Programming and Basic Mathematical skills

What you can get from this course

- Why protect? What protect? How protect?
- Sorts of threats against modern computers and networks
  - Network attacks, types of worms and viruses
- How the above problems is being solved in the industry
  - Concepts of encryption, hardware and software protection (firewall, IDS, policies and procedures)

Syllabus at a glance

- Basic terminology.
- Classical Encryption. Early cryptography. Rotor machines: Enigma and its relatives.
- Block ciphers and the Data Encryption Standard. AES
- Basic concepts in Number Theory and Finite Fields
- Public Key Cryptography and RSA.
- Cryptographic Hash Function
- Digital Signatures and Certificates
- User Identification and Authentication
- Access Control (Authorization)
- Network Firewalls
- Intrusion Detection System

How to take this course: reading

Basic literature (Required Reading!):

- Cryptography and Network Security by William Stallings, 5th edition, 2006
- Security in Computing by Charles P. Pfleeger and Shari Lawrence Pfleeger, 4th edition, 2006

How to take this course: schedule

- Attend all lectures
- Submit assignments on time
  - Do not leave until the last minute
  - Marks will be deducted for late submission **(-20% for each day)**
  - Cannot mark what is not there
  - **Plagiarism** … will be detected!
    - For the **1st time**, chance will be given with 50% of the total mark
- See assignment description for submission date

Assessment

- Overall mark:
  - 30% - 1st term
  - 30% - 2nd term
  - 40% - Final Examination

The final version of grading policy will be available soon.

Questions?

Basic Concepts and Terminology

- Vulnerability
- Threat
- Attack
- Security concepts:
  - Confidentiality, Integrity, Availability
- Security Service

Vulnerability

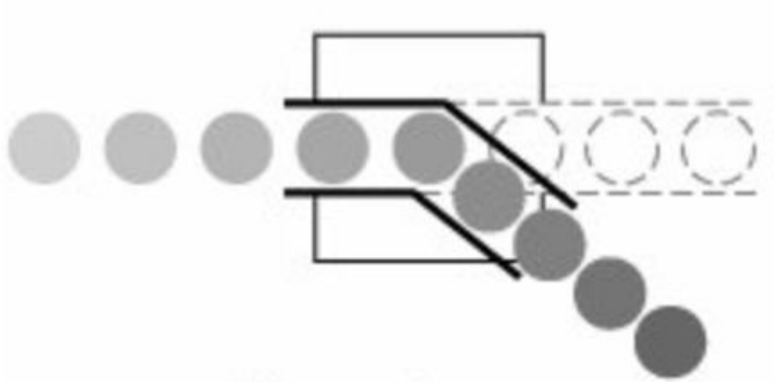
- Some state of the system of being open to attacks or injuries.
- Example in house analogy:
  - “Open Door” is the vulnerability for thieves

Threat

- A statement of an intention to injure, damage or any other enemy action.
- A potential for violation of security.
- In case of “house” example:
  - “Loss of Money” is a threat

- 4 kind of threats:
  - Interception
  - Interruption
  - Modification
  - Fabrication

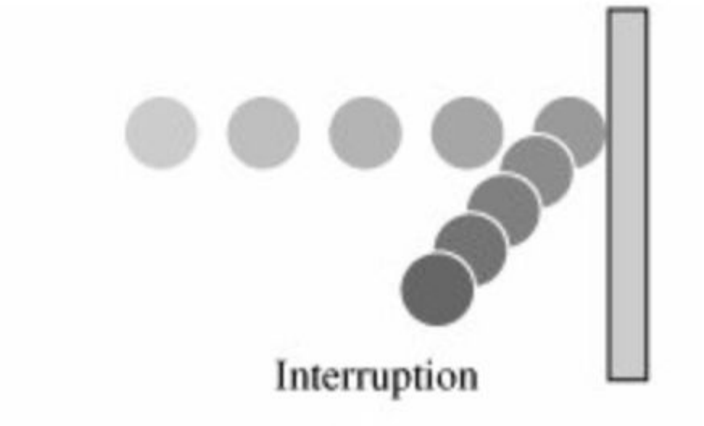
- **Interception** – unauthorized access to a data.
- For example,
  - Illegal copying of program or data files



Interception

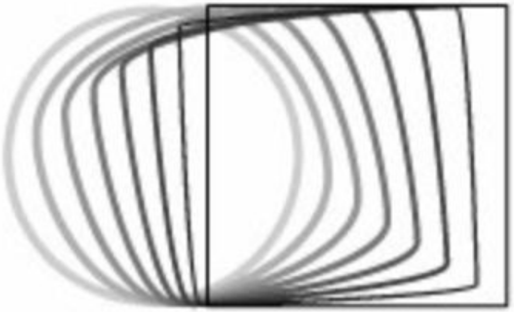
Source: https://genesisdatabase.wordpress.com/

- **Interruption** – a data of the system becomes lost, unavailable, or unusable.
- Examples include
  - Erasure of a program or data file
  - Malicious destruction of a hardware device



Source: https://genesisdatabase.wordpress.com/

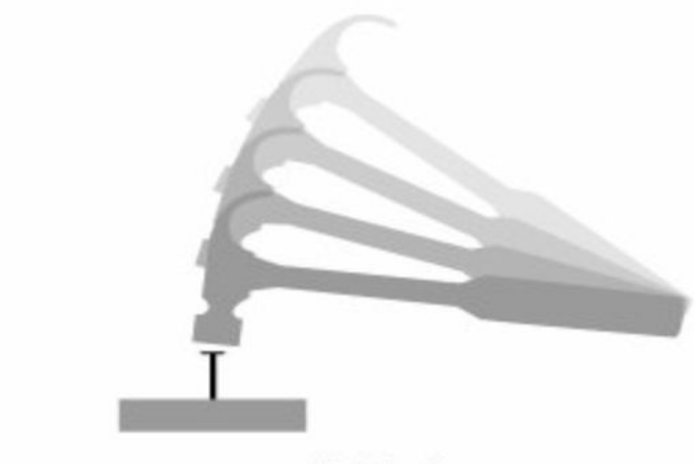
- **Modification** – unauthorized, change tamper with a data.
- For example,
  - Someone might change the values in a database



Modification

Source: https://genesisdatabase.wordpress.com/

- **Fabrication** – E.g. Unauthorized insertion to a existing database.



Fabrication

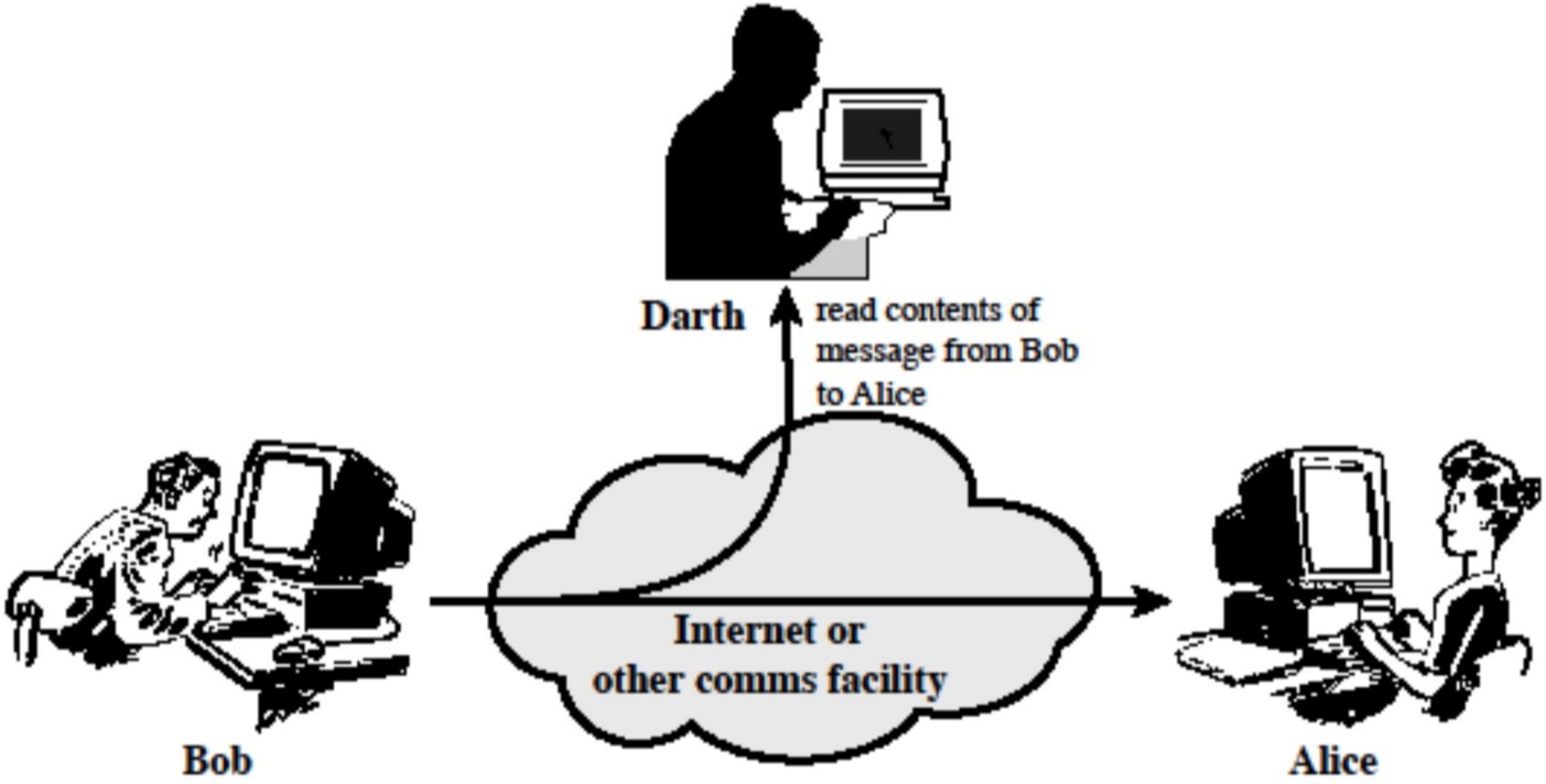
Source: https://genesisdatabase.wordpress.com/

Attack

- An assault on system security
- A deliberate attempt to evade security services

- Kind of attacks:
  - Passive attacks
  - Active attacks

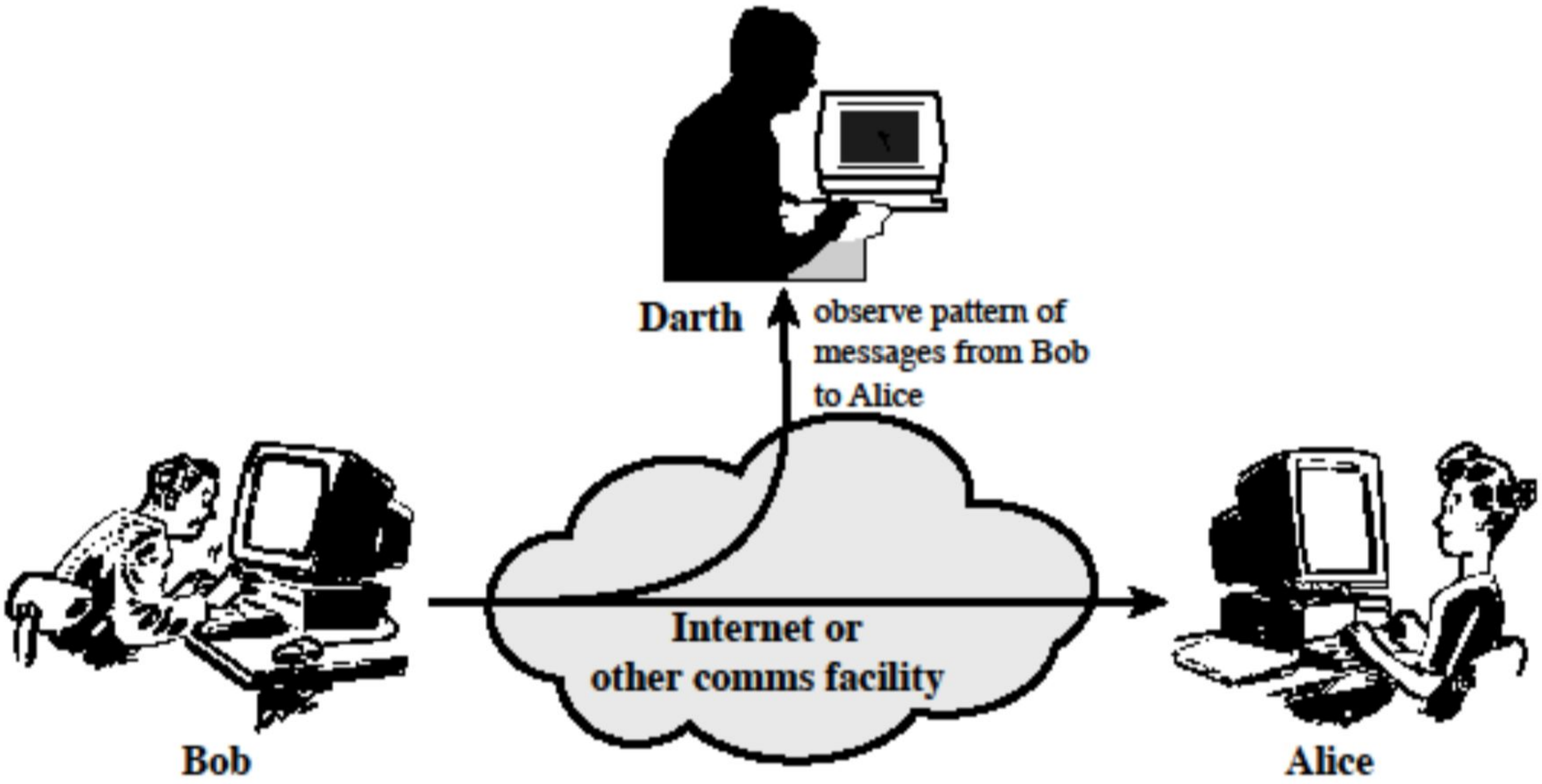
Passive Attacks


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

(a) Release of message contents

Source: Cryptography and Network Security by Stallings

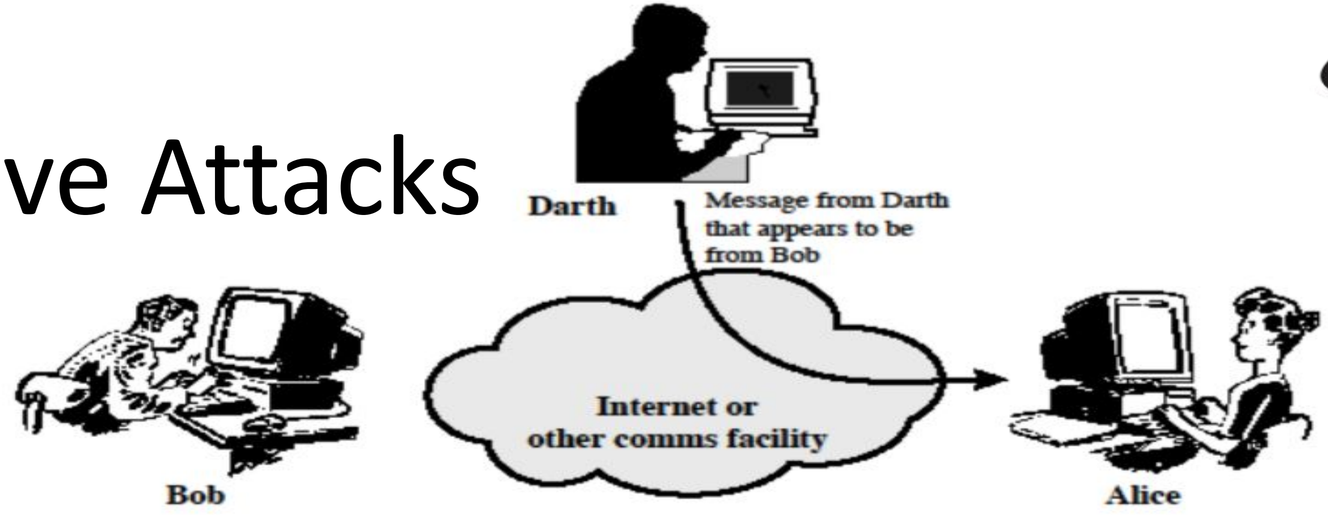
Passive Attacks (cont.)


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

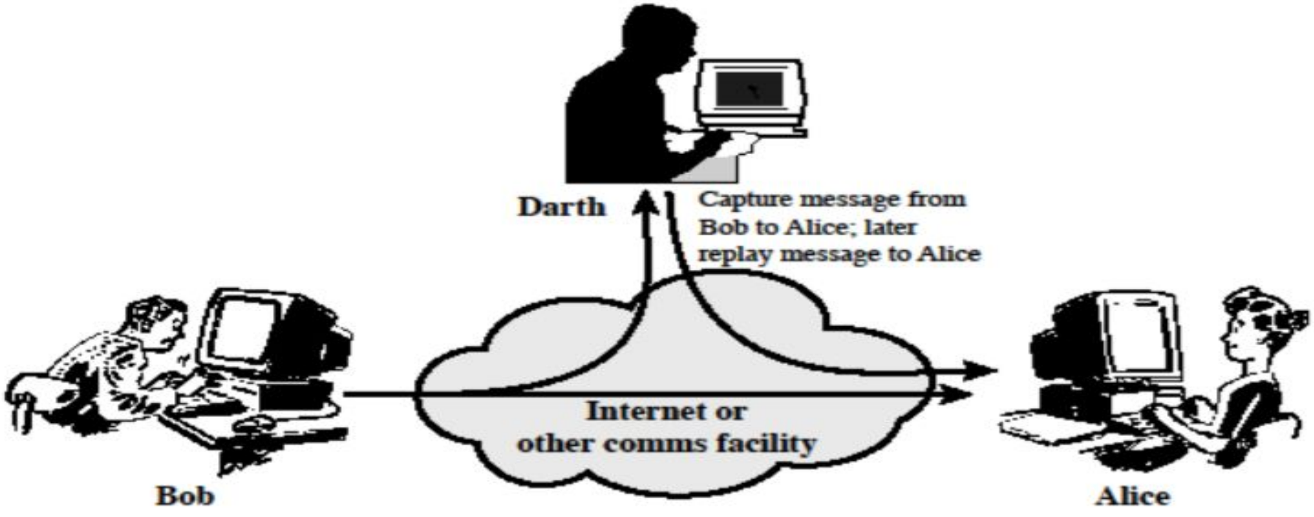
(b) Traffic analysis

Source: Cryptography and Network Security by Stallings

Active Attacks


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

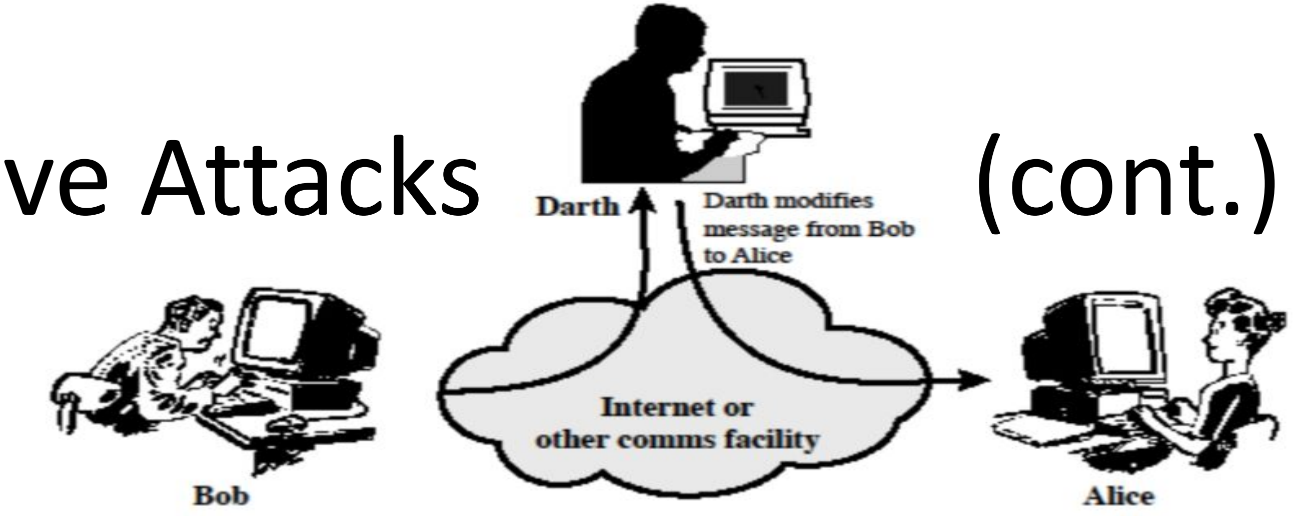
(a) Masquerade


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

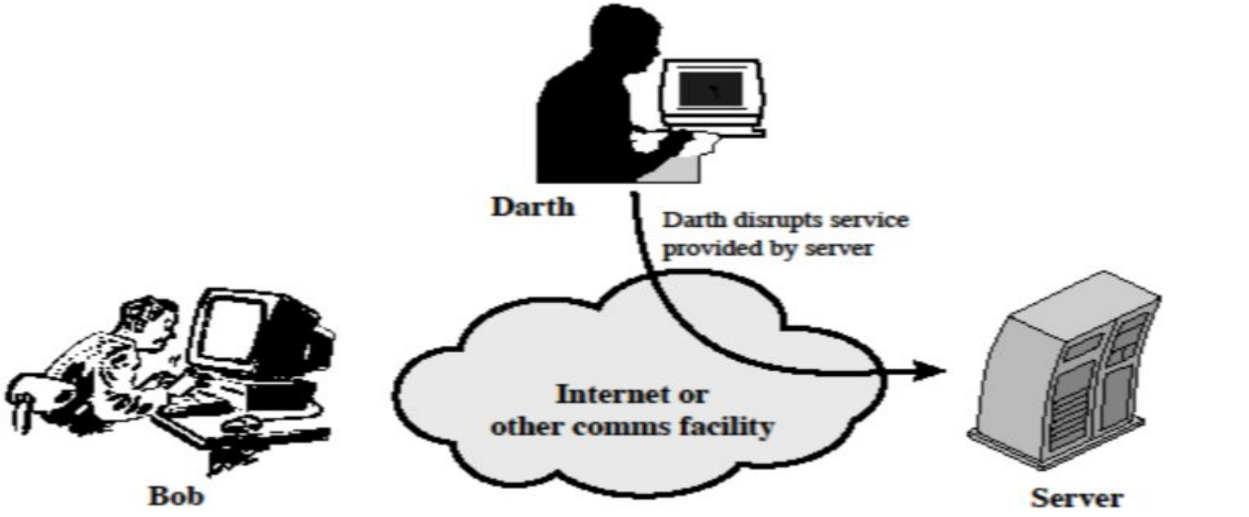
(b) Replay

Source: Cryptography and Network Security by Stallings

Active Attacks (cont.)


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages


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

(d) Denial of service

Source: Cryptography and Network Security by Stallings

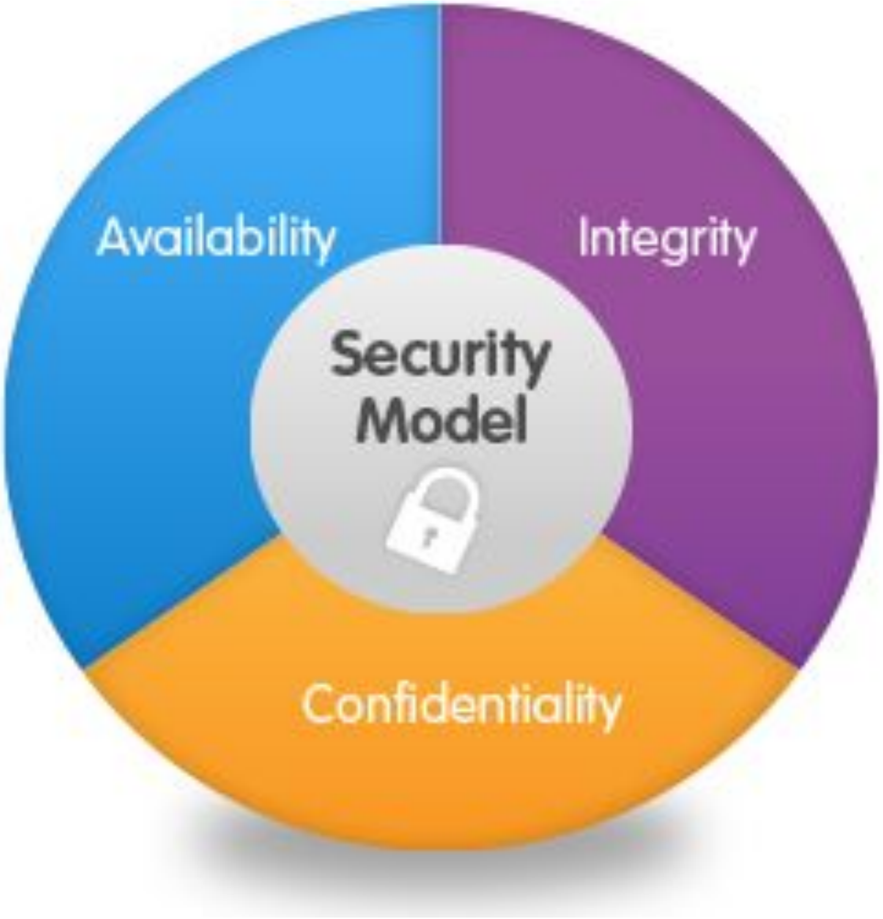
Why to attack? (MOM)

- **M**ethod: skills, knowledge, tools, etc.
- **O**pportunity: time and access
- **M**otive: fame, money, etc.

Key Security Concepts

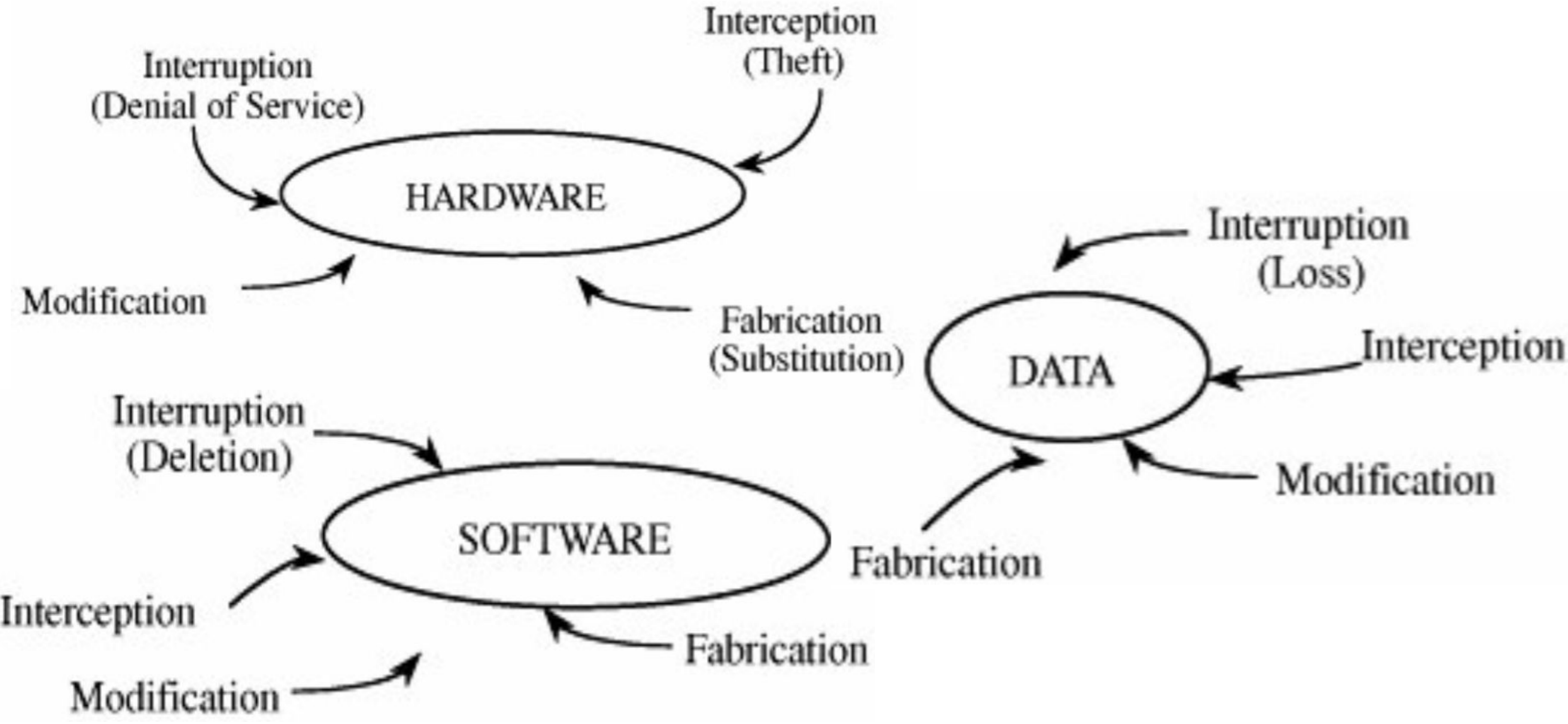
- Used to prevent weaknesses from being exploited
  - ***C*onfidentiality** – access only by authorized users; E.g. Student grades
  - ***I*ntegrity** – modify only by authorized users; E.g. Patient information
  - ***A*vailability** – E.g. Users want to check their accounts

Relationship between Confidentiality, Integrity, and Availability

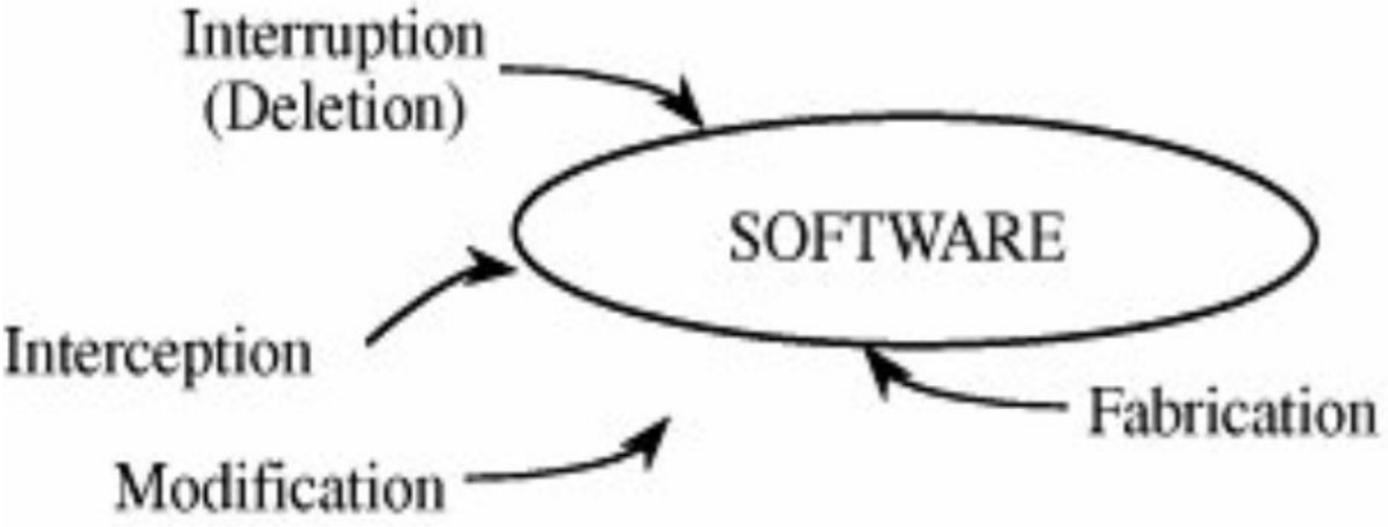


How to avoid security attacks?

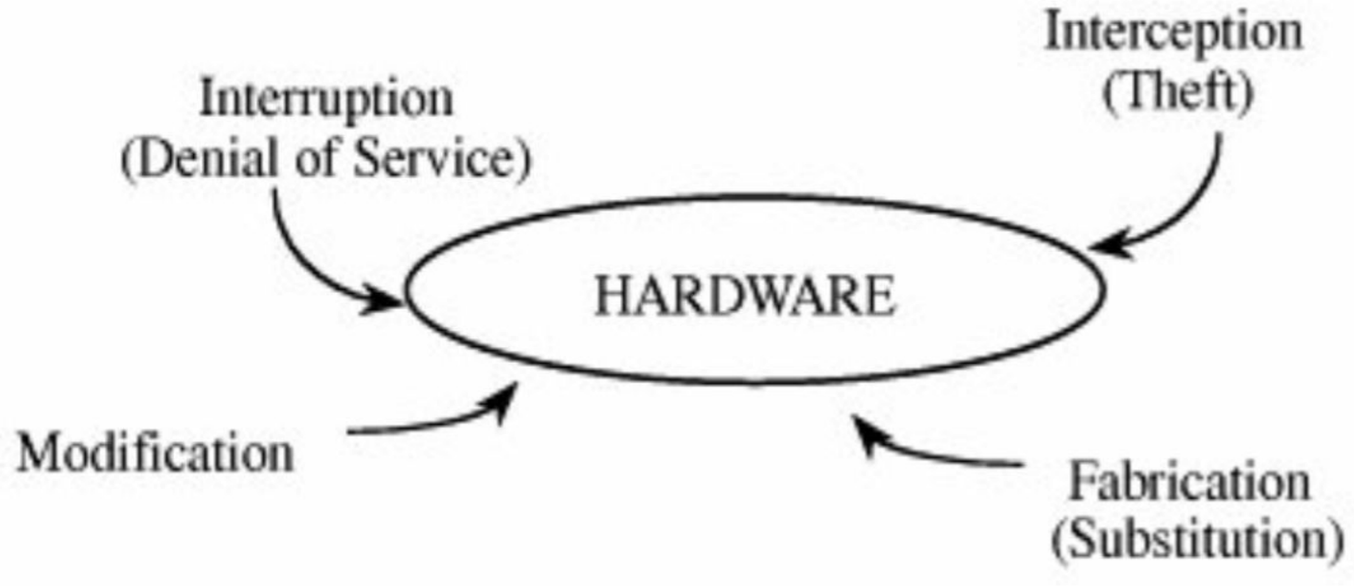
- Think about vulnerabilities



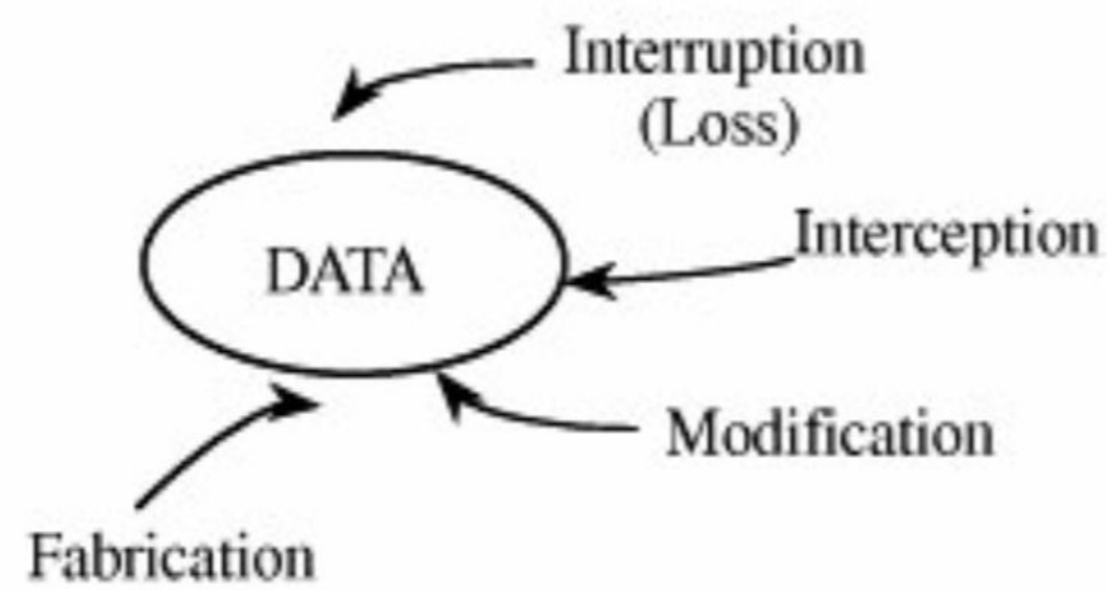
- Viruses, worms, trojans



- Servers, server rooms, laptops, etc. (Physical Security)



- Data protection
  - The most important thing in majority of information systems



How to protect? 3Ds of Security

- ***D*****efense** – reducing risks and saving costs of incidents (E.g. Firewalls, antivirus software, spam filters, etc.)
- ***D*****eterrence** – punishing makes attackers think twice (E.g. Laws, organizational policies and procedures)
- ***D*****etection** – need alert if security incident occurs (E.g. Audit logs, intrusion detection system, network traffic monitoring)

How to protect? 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
  - E.g. have signatures, dates; need protection from disclosure

Security Services

- X.800:
  - “a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”
- RFC 2828:
  - “a processing or communication service provided by a system to give a specific kind of protection to system resources”

Security Services (X.800)

- **Authentication** – assure that communication entity is the one claimed
- **Access Control** – prevention of the unauthorized use of a resource
- **Data Confidentiality** – protection of data from unauthorized disclosure
- **Data Integrity** – assure 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 (X.800)

- Features designed to protect, prevent, or recover from a security attack
- No single mechanism that will support all services required
- Specific security mechanisms:
  - Encipherment, digital signatures, access controls, data integrity, authentication

Summary

- Basic Information Security Terminology
- Key Security Concepts
  - **C**onfidentiality, **I**ntegrity, **A**vailability
- Subject of attacks? Hardware, Software and Data
- How to avoid attacks?
  - Think about vulnerabilities
- How to protect?
  - 3 Ds: **D**efense, **D**eter, **D**etect
  - Security Services

Reading

- Cryptography and Network Security by Stallings
- Chapter 1:
  - Sections 1.1, 1.3, 1.4, 1.5, 1.8

Questions?