Chapter 1

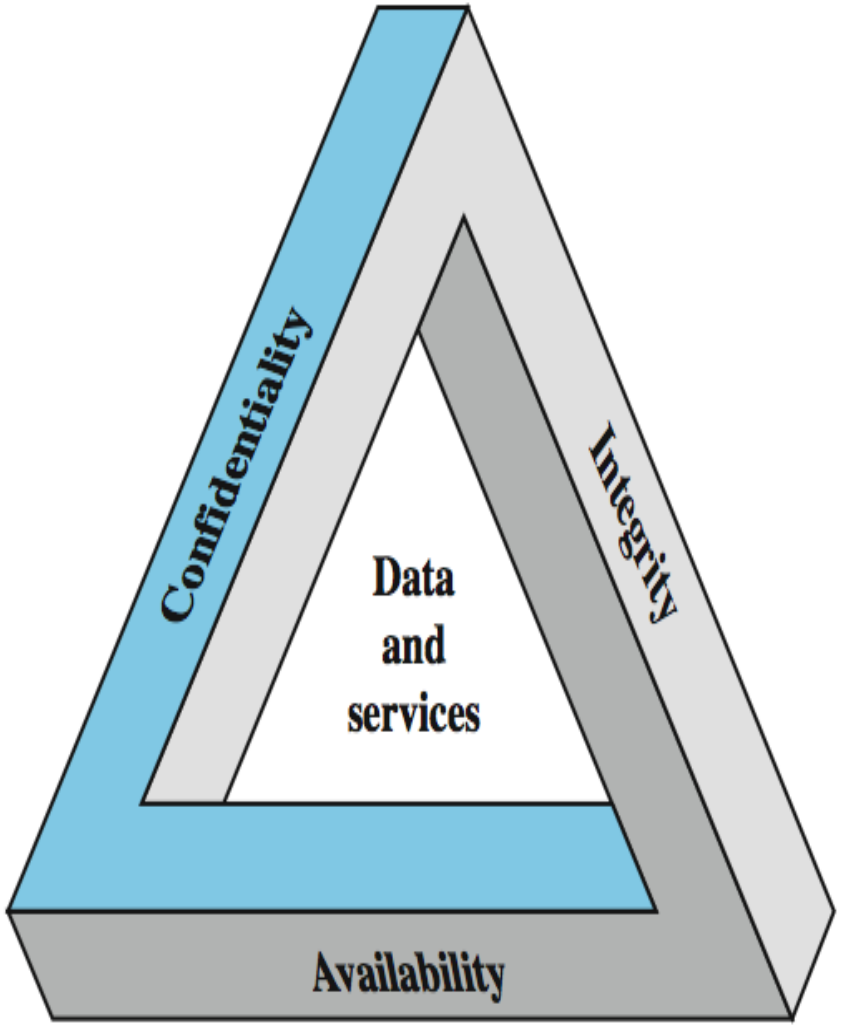
Introduction and mathematics of cryptography

Objectives

- To define three security goals
- To define security attacks that threaten security goals
- To define security services and how they are related to the three security goals
- To define security mechanisms to provide security services
- To introduce two techniques, cryptography and steganography, to implement security mechanisms.

Computer Security

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information and telecommunication) NIST 1995].



Three Key Objectives

- Confidentiality (student grades)
  - Data confidentiality
  - Privacy
- Integrity (patient information)
  - Data integrity
  - System integrity
- Availability (authentication service)
- Additional concepts
  - Authenticity
  - Accountability

Computer Security Challenges

- Not simple
- Must consider potential attacks
- Procedures used counter-intuitive
- Involve algorithms and secret info
- Must decide where to deploy mechanisms
- Not perceived on benefit until fails
- Requires regular monitoring
- Too often an after-thought
- Regarded as impediment to using system

Aspects of Security

- 3 aspects of information security:
  - **security attack**
  - **security mechanism:** detect, prevent, recover
  - **security service**
- terms
  - *threat* – a potential for violation of security
  - *attack* – an assault on system security, a deliberate attempt to evade security services

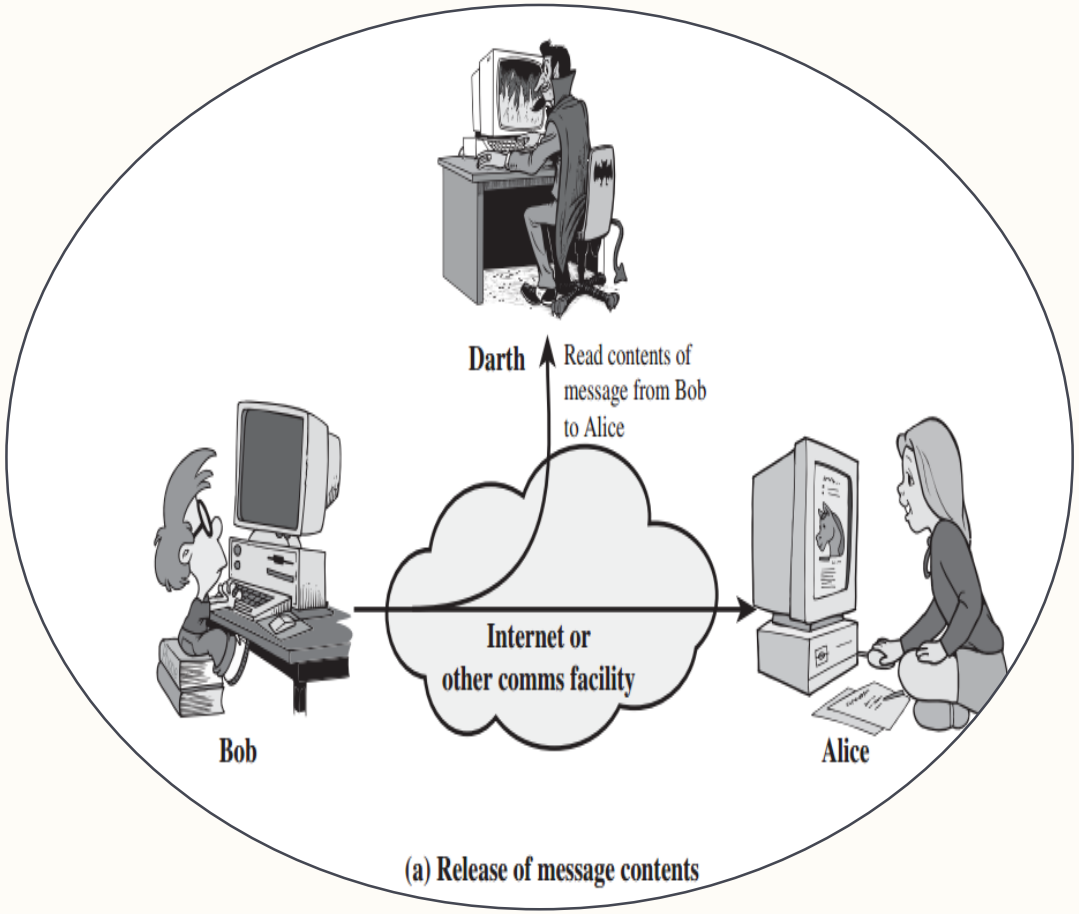
Cryptographic Attacks

The attacks are classified into two types:

- ***Passive attacks*** do not involve any modifications to the contents of an original message
  - Release of message content
  - Traffic analysis
- In ***Active attacks*** the contents of the original message are modified in some way.
  - Masquerade
  - Modification of message
  - Replay
  - Denial of sevice

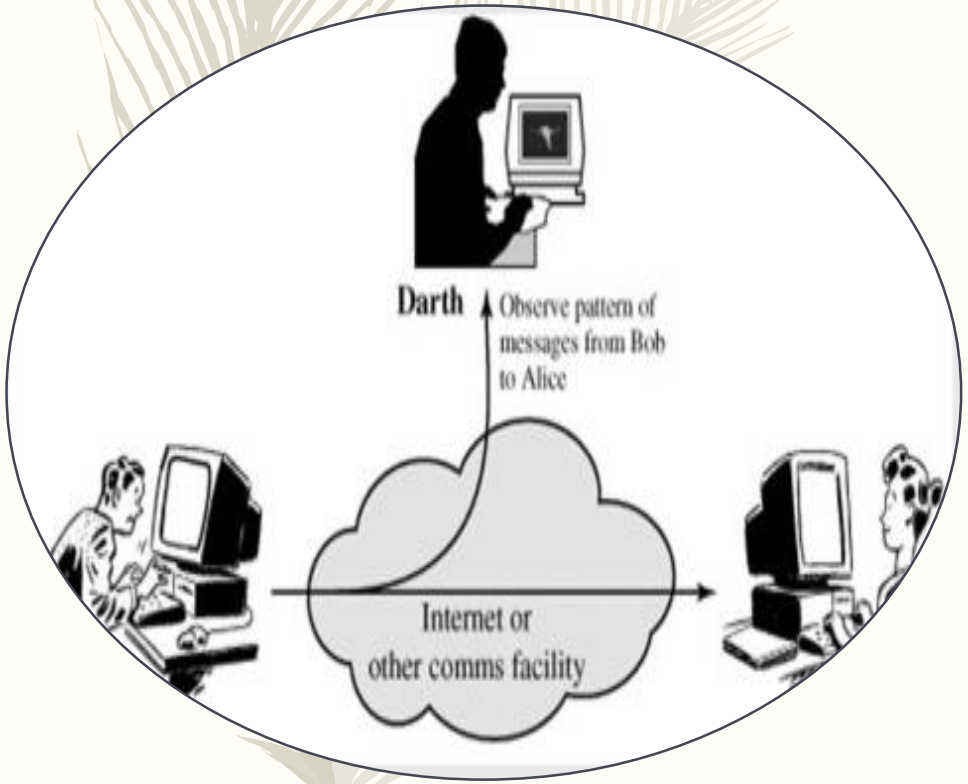
Passive Attacks (1)
Release of Message Contents

A passive attack **monitors the contents** of the transmitted data. When the messages are exchanged neither the sender nor the receiver is aware that a third party may capture the messages.



(a) Release of message contents

Passive Attacks (2)
Traffic Analysis

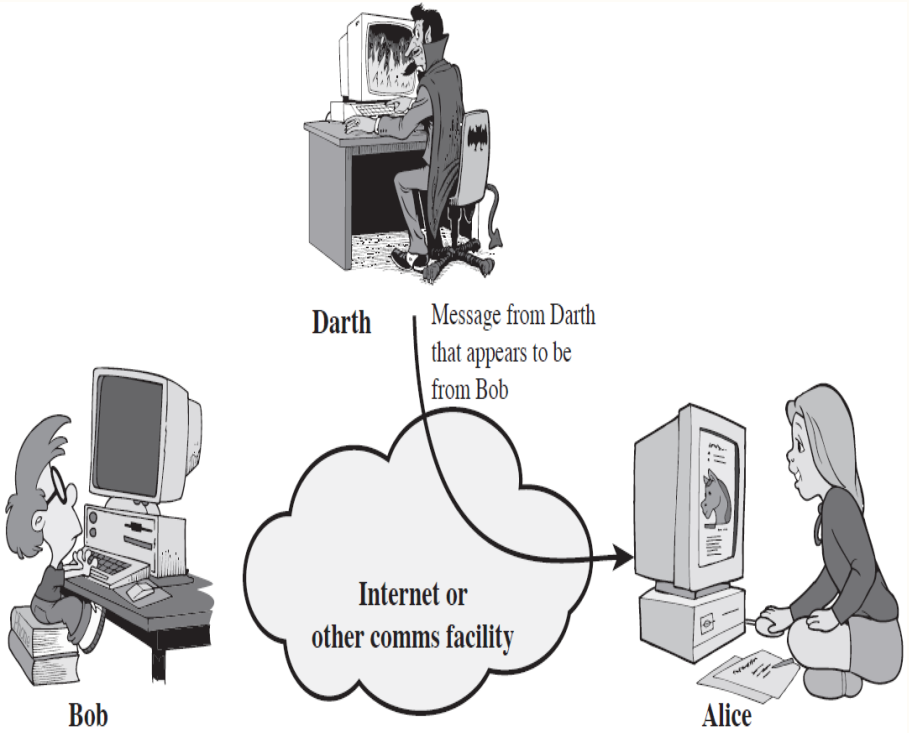


Traffic analysis is the process of **intercepting and examining messages** in order to deduce information from **patterns in communication.**

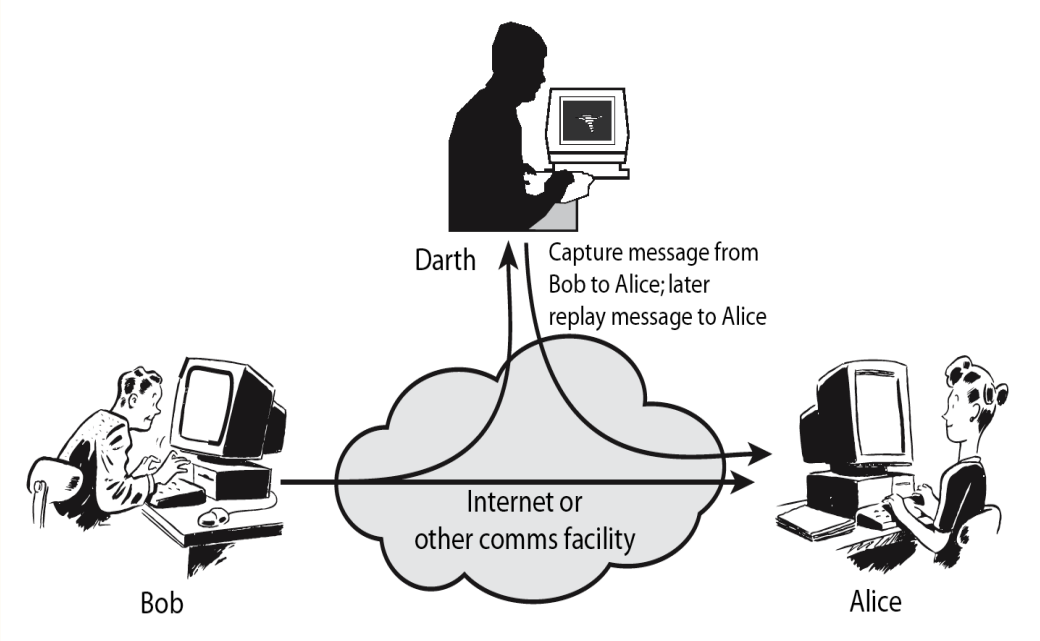
- Passive attacks do not affect system resources
  - Eavesdropping, monitoring
- Two types of passive attacks
  - Release of message contents
  - Traffic analysis
- Passive attacks are very difficult to detect
  - Message transmission apparently normal
    - *No alteration of the data*
  - Emphasis on prevention rather than detection
    - *By means of encryption*

Active Attacks (1) Masquerade

A masquerade attack is any attack that uses a **forged identity** (such as a network identity) to **gain unofficial access** to a personal or organisational computer.



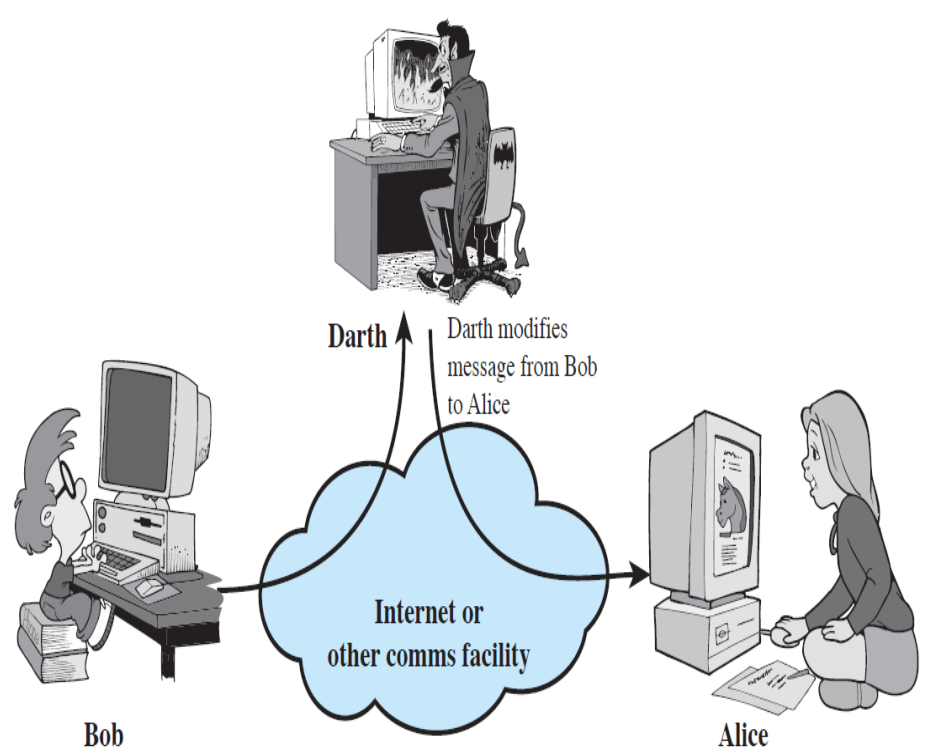
Active Attacks (2) Replay



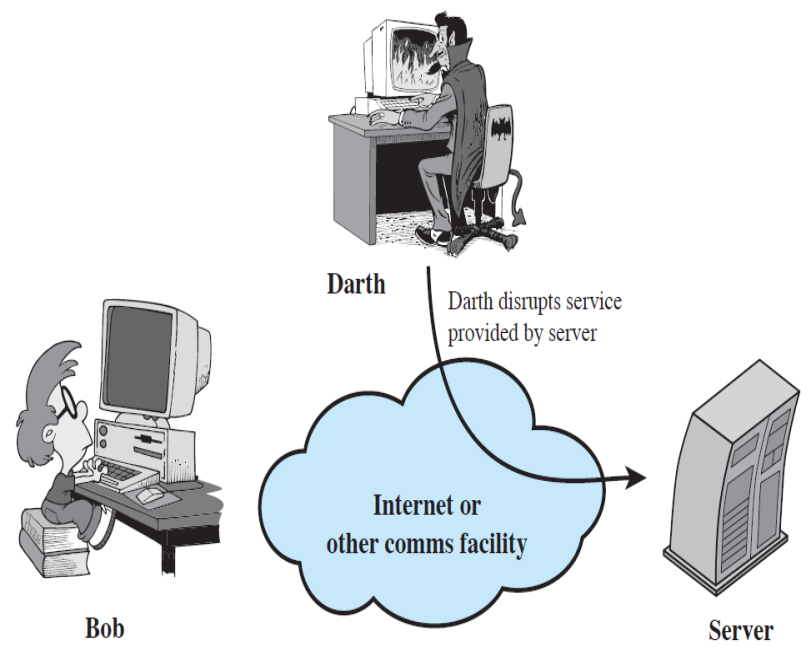
A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is **maliciously or fraudulently repeated** or delayed.

Active Attacks (3)
Modification of Messages

In a message modification attack, an intruder **alters packet header addresses** to direct a message to a different destination or **modify the data** on a target machine. …



Active Attacks (4)
Denial of Service



A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it **inaccessible to its intended users**.

- Active attacks try to alter system resources or affect their operation
  - Modification of data, or creation of false data
- Four categories
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service: preventing normal use
    - *A specific target or entire network*
- Difficult to prevent
  - The goal is to detect and recover

Model for Network Security