# Lecture 1
# Information Security

**Cybersecurity** is the protection of information that is stored, transmitted, and processed in a networked system of computers, other digital devices, and network devices and transmission lines, including the Internet. Protection encompasses confidentiality, integrity, availability, authenticity, and accountability. Methods of protection include organizational policies and procedures, as well as technical means such as encryption and secure communications protocols.

"الأمن السيبراني هو حماية المعلومات التي يتم تخزينها ونقلها ومعالجتها في نظام موصول من أجهزة الكمبيوتر
والأجهزة الرقمية الأخرى وأجهزة الشبكة وخطوط النقل، بما في ذلك الإنترنت. تشمل الحماية السرية والنزاهة والتوافر
والأصالة والمساءلة. تشمل أساليب الحماية السياسات والإجراءات التنظيمية، بالإضافة إلى الوسائل الفنية مثل التشفير
وبروتوكولات الاتصالات الآمنة"

As subsets of cybersecurity, we can define the following:

■ **Information security**: This term refers to preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved.

■ **Network security**: This term refers to protection of networks and their service from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects

**Security Objectives**:

The cybersecurity definition introduces three key objectives that are at the heart of information and network security:

1. **confidentiality**: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
2. **integrity**: Assures that data (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.
3. **Availability**: Assures that systems work promptly and service is not denied to authorized users

These three concepts form what is often referred to as the CIA triad as figure below:

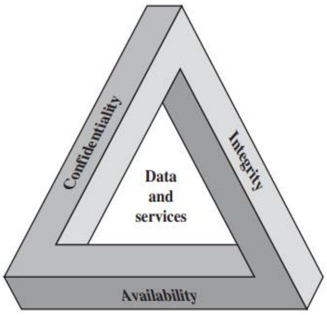
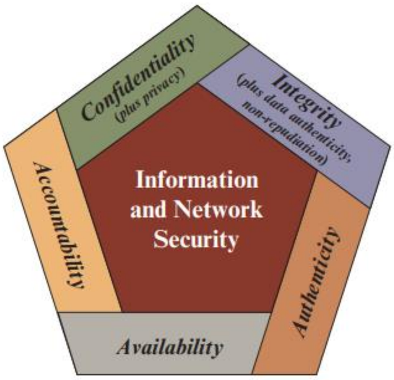


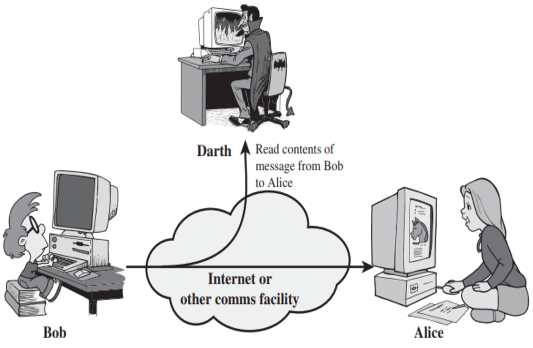
Figure 1.1 The Security Requirements Triad

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture.Two of the most commonly mentioned are as follows:

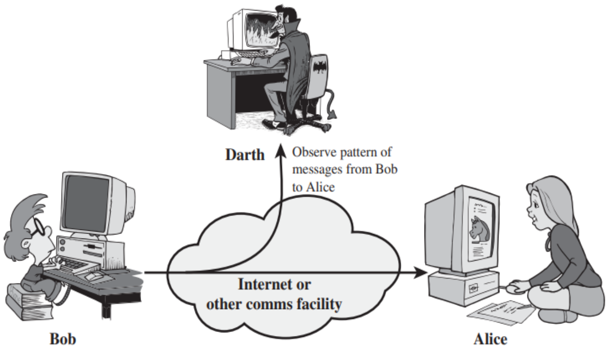
- **Authenticity**: confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability** in the context of security refers to the principle that actions taken by individuals or entities can be traced back to them. This concept is crucial for ensuring that users and systems are held responsible for their actions, especially in environments where security breaches can occur.



- Security Attacks:
    1. **Passive attacks**: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.

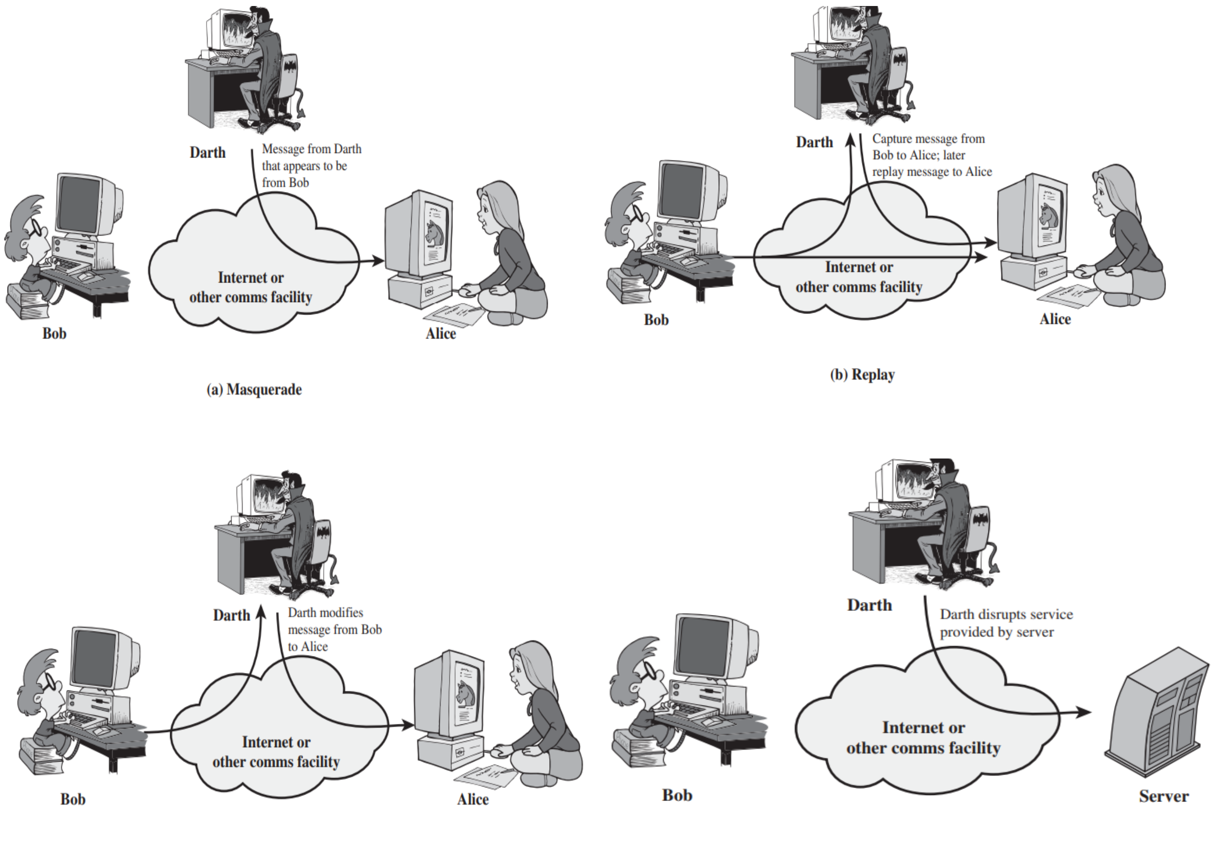

Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents


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

(b) Traffic analysis

2. **Active attacks**: Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories.


Darth
Message from Darth that appears to be from Bob
Bob
Internet or other comms facility
Alice
Darth
Capture message from Bob to Alice; later replay message to Alice
Bob
Internet or other comms facility
Alice
Darth
Darth modifies message from Bob to Alice
Bob
Internet or other comms facility
Alice
Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

(a) Masquerade

(b) Replay

(c) Modification of messages

(d) Denial of service