Chapter 1
Information and Network Security Concepts

1. Cybersecurity, Information Security, And Network 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.
    - **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:

- **Confidentiality:** This term covers two related concepts:
    - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
    - **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- **Integrity:** This term covers two related concepts:
    - **Data integrity:** Assures that data (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner. This concept also encompasses **data authenticity**, which means that a digital object is indeed what it claims to be or what it is claimed to be, and nonrepudiation, which is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of

the sender's identity, so neither can later deny having processed the information.

- **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

- **Availability:** Assures that a system performs its intended function in an unimpaired manner.

These three concepts form what is often referred to as the **CIA 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 (Figure 1.1). Two of the most commonly mentioned are as follows:

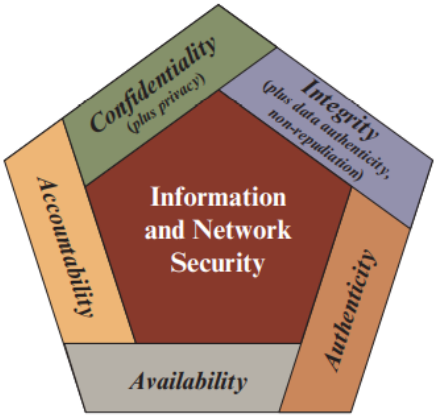

Figure 1.1 Essential Information and Network Security Objectives

- **Authenticity:** verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence[1], fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

[1] The concept of deterrence is that people choose not to act in a specific way because they are afraid of what will happen if they do.

2. The OSI Security Architecture

ITU-T Recommendation X.800, Security Architecture for OSI, defines such a systematic approach to assess effectively the security needs of an organization and to evaluate and choose various security products and policies. The OSI security architecture focuses on **security attacks**, **mechanisms**, and **services**. These can be defined briefly as:

- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

In the literature, the terms threat and attack are commonly used, with the following meanings:

- **Threat:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- **Attack:** Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

A useful means of classifying security attacks, used both in X.800, is in terms of **passive attacks** and **active attacks**. *A passive attack* attempts to learn or make use of information from the system but does not affect system resources. *An active attack* attempts to alter system resources or affect their operation.

  - **Passive attacks** are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the attacker is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.
  - **Active attacks** involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: replay, masquerade, modification of messages, and denial of service.
    - A masquerade takes place when one entity pretends to be a different entity.
    - Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
    - The denial of service prevents or inhibits the normal use or management of communication facilities.

3. Security Services

A security service is a capability that supports one or more of the security requirements (confidentiality, integrity, availability, authenticity, and accountability). The most important security services are summarized below.

- **Authentication**: The authentication service is concerned with assuring that a communication is authentic. Two specific authentication services are defined in X.800:
    - **Peer entity authentication**: Provides for the corroboration of the identity of a peer entity in an association. Two entities are considered peers if they implement the same protocol in different systems; for example, two TCP modules in two communicating systems. Peer entity authentication is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.
    - **Data origin authentication:** Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail, where there are no ongoing interactions between the communicating entities.
- **Access Control**: In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links.
- **Data Confidentiality:** is the protection of transmitted data from passive attacks.
- **Data Integrity:** As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.
- **Nonrepudiation:** prevents either sender or receiver from denying a transmitted message.
- **Availability Service:** Availability is the property of a system, or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).