Chapter 2

Security Attack, Services and Mechanism

Introduction:

With the introduction of the computer, the need for automatic tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, such as a time-sharing system, and the need is even more acute for systems that can be accessed over a public telephone network, data network, or the Internet. The generic name for the collection of tools designed to protect data and to thwart hackers is **computer security**. The second major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer.

Network security measures are needed to protect data during their transmission. internet security, which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information. Consider the following example of security violations: *User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.*

1.1 The OSI Security Architecture

To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. ITU-T Recommendation X.800, ***Security Architecture for OSI***, defines such a systematic approach. The OSI security architecture is useful to managers as a way of organizing the task of providing security.

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:

- **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.

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Attack: An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

1.2 Security Attacks

A useful means of classifying security attacks, 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:

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. Two types of passive attacks are ***release of message contents and traffic analysis.***

- The **release of message contents** is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
- A second type of passive attack, **traffic analysis**, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, ***the emphasis in dealing with passive attacks is on prevention rather than detection.***

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:

1. ***masquerade,***
2. ***replay,***
3. ***modification of messages, and***
4. ***denial of service.***

- A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

- **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

- **denial of service** prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention. Figure 1 shows the passive and active attack types.

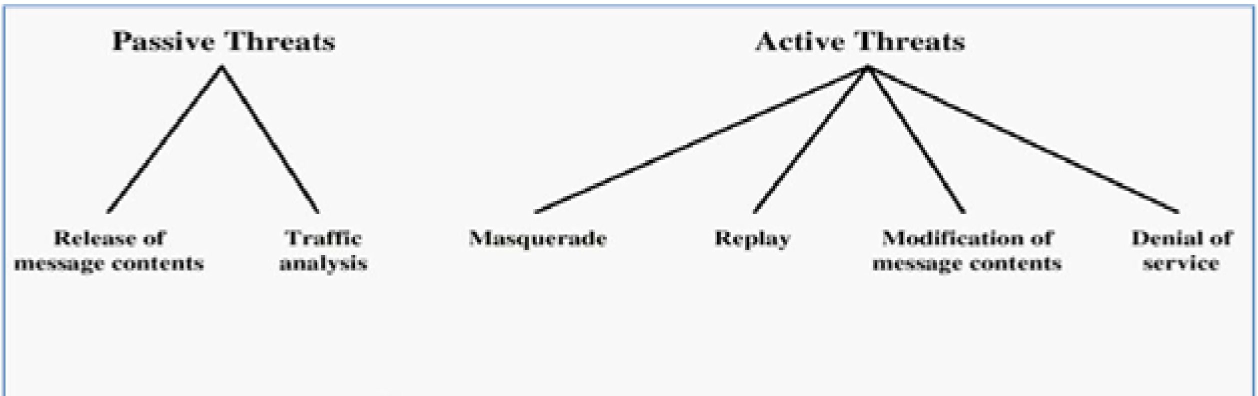


Figure 1 Active and Passive Security Threats

Figure1: Active and passive threats

1.3 Security Services

X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers. Perhaps a clearer definition is: *a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.*

1.3.1 Authentication

The authentication service is *concerned with assuring that a communication is authentic*. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. *First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception*. 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. It 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 prior interactions between the communicating entities.

1.3.2 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*. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

1.3.3 Data Confidentiality

Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. *The broadest service protects all user data transmitted between two users over a period of time*. For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. These refinements are less useful than the broad approach and may even be more complex and expensive to implement.

The other aspect of confidentiality is the *protection of traffic flow from analysis*. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

1.3.4 Data Integrity

As with confidentiality*, integrity can apply to a stream of messages, a single message, or selected fields within a message.* Again, the most useful and straightforward approach is total stream protection. *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.*

We can make a distinction between *the service with and without recovery*. Because the integrity service relates to active attacks, we are concerned with detection rather than prevention. If a violation of integrity is detected, then the service may simply report this violation, and some other portion of software or human intervention is required to recover from the violation. Alternatively, there are mechanisms available to recover from the loss of integrity of data, as we will review subsequently. The incorporation of automated recovery mechanisms is, in general, the more attractive alternative.

1.3.5 Nonrepudiation

Nonrepudiation *prevents either sender or receiver from denying a transmitted message*. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

1.4 Security Mechanisms

Following is the list of the security mechanisms defined in X.800. As can be seen the mechanisms *are divided into those that are implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service*.

X.800 distinguishes between reversible encipherment mechanisms and irreversible encipherment mechanisms. *A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.*

A. Specific Security Mechanisms

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

1. Encipherment: *The use of mathematical algorithms to transform data into a form that is not readily intelligible.* The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
2. 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).
3. Access Control: *A variety of mechanisms that enforce access rights to resources*.
***4.* Data Integrity:** A variety of mechanisms used to *assure the integrity of a data unit or stream of data units.*
***5.* Authentication Exchange:** A mechanism *intended to ensure the identity of an entity by means of information exchange.*
***6.* Traffic Padding:** The *insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.*
7. Routing Control: *Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected*.
8. Notarization: *The use of a trusted third party to assure certain properties of a data exchange*.

B. Pervasive Security Mechanisms

Mechanisms that are not specific to any particular OSI security service or protocol layer.
1. Trusted Functionality: *That which is perceived to be correct with respect to some criteria* (e.g., as established by a security policy).
2. Security Label: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
3. Event Detection: Detection of security-relevant events.
4. Security Audit Trail: Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
5. Security Recovery: Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

1.5 A Model for Network Security

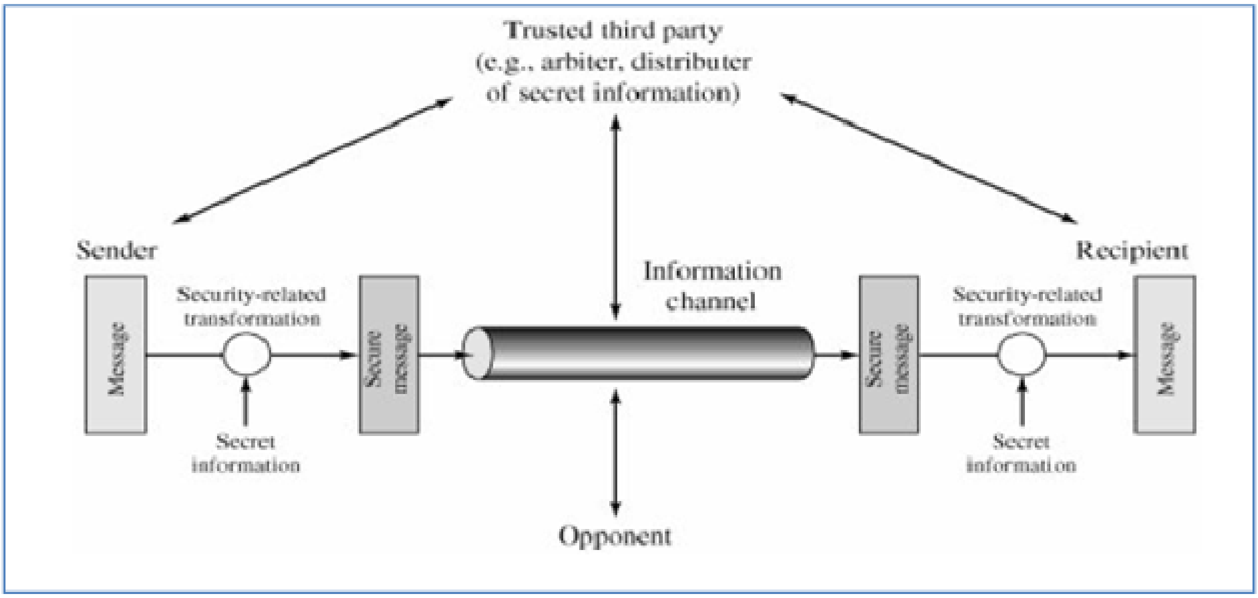
A model for much of what we will be discussing is captured, in very general terms, in Figure 2. A message is to be transferred from one party to another across some sort of internet. *The two parties, who are the principals in this transaction, must cooperate for the exchange to take place*. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

● *A security-related transformation on the information to be sent.* Examples include ***the encryption of the message***, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

● Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

Figure 2: Model for network security



A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. *Design an algorithm for performing the security-related transformation*. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate *the secret information* to be used with the algorithm.
3. Develop *methods for the distribution and sharing of the secret information*.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. Or, the intruder can be a disgruntled employee who wishes to do damage, or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers). Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers. Programs can present two kinds of threats:

● **Information access threats** intercept or modify data on behalf of users who should not have access to that data.

● **Service threats** exploit service flaws in computers to inhibit use by legitimate users.

Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.

The security mechanisms needed to cope with unwanted access fall into two broad categories. The first category might be termed a *gatekeeper function*. It includes ***password-based login procedures t***hat are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that *monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.*