# Unit 1: Introduction to Information Security

**Basic concepts of information security:**

**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 a 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.

**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. This is difficult enough in a centralized data processing environment; with the use of local and wide area networks, the problems are compounded.

The OSI security architecture is useful to managers as a way of organizing the task of providing security. Furthermore, because this architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.

**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.

**Security Attacks**

**Security Attacks:** An attack is an action that comprises the information or networksecurity.

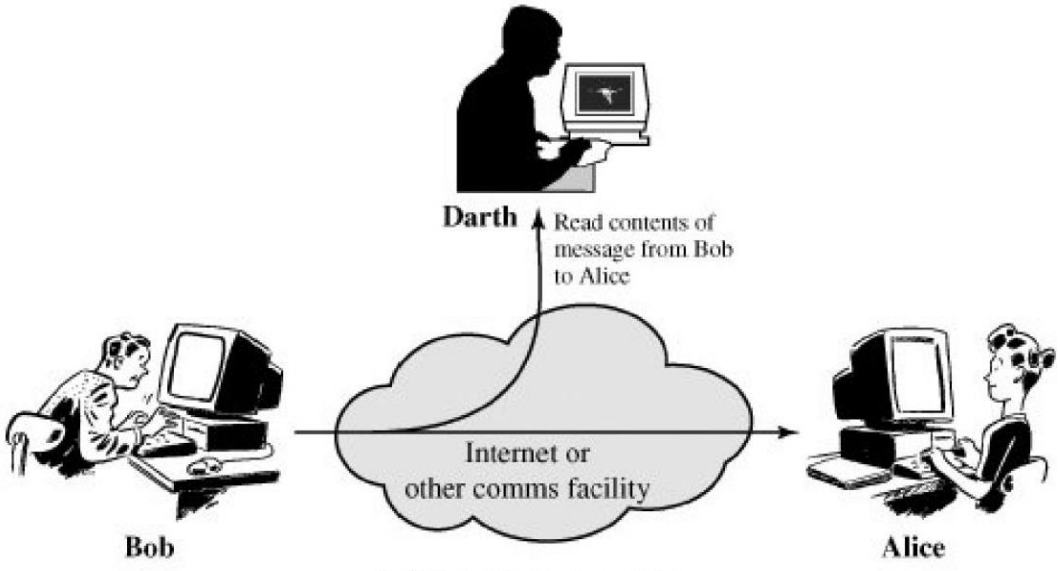
There are two types of attacks:

1. Passive Attack
2. Active Attack

**Passive Attack**

The attacker only monitors the traffic attacking the confidentiality of the data. It contains release of message contents and traffic analysis (in case of encrypted data).

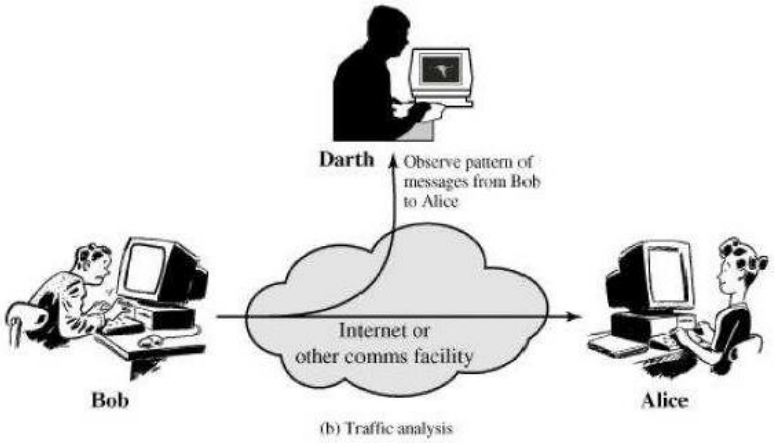
1. **Release of message contents:**
   - The release of message contents is easily understood.
   - A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
   - We would like to prevent an opponent from learning the contents of these transmissions.




(a) Release of message contents

2. **Traffic analysis:**
   - A second type of passive attack, traffic analysis.
   - Suppose that we had a way of masking the contents of messages or other information.
   - 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 send and received in an apparently normal fashion and the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

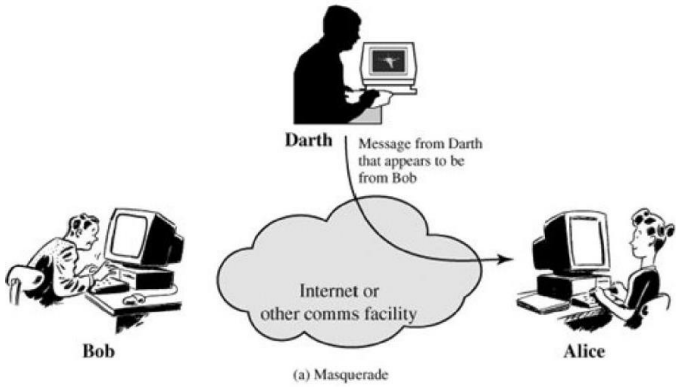


(b) Traffic analysis

**Active attack**

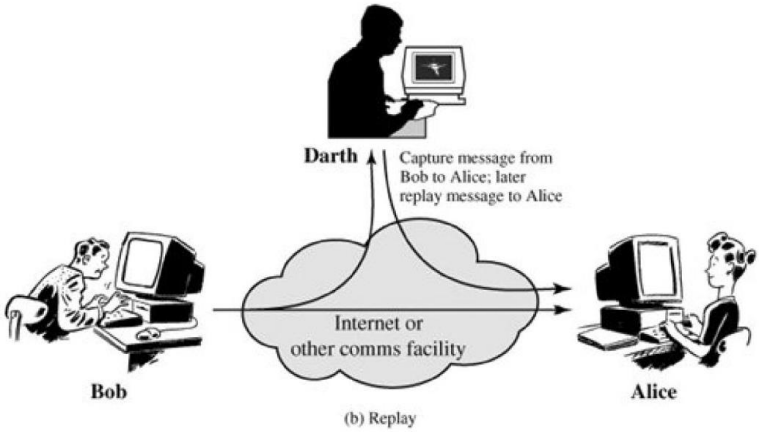
Attacker tries to alter transmitted data. It includes masquerade, modification, replay and denial of service.

1. **Masquerade:** A masquerade takes place when one entity pretends to be a different entity (Figure a). A masquerade attack usually includes one of the other forms of active attack.



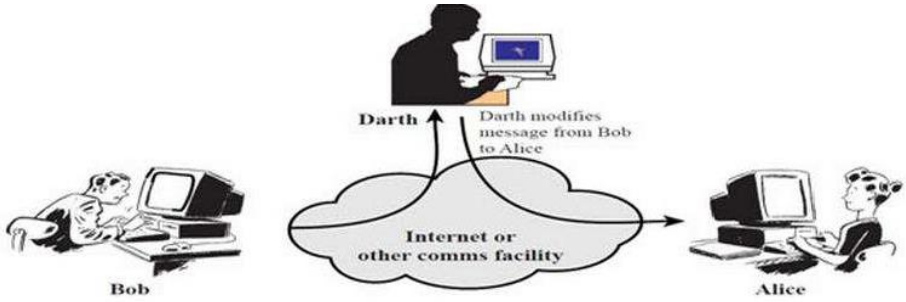
(a) Masquerade

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



(b) Replay

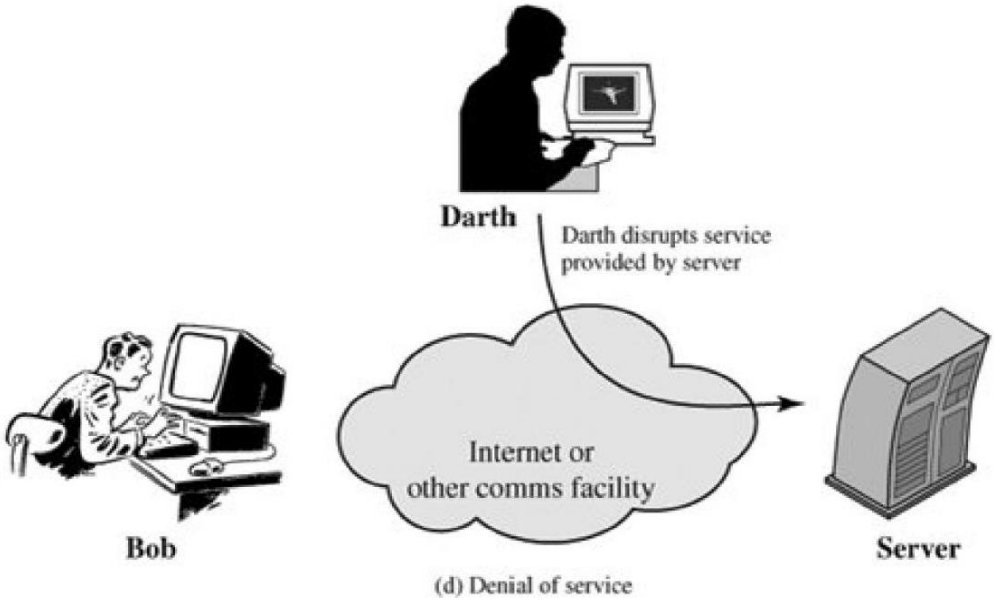
3. **Modification of messages:**
   - Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure c).
   - For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."



(c) Modification of messages

4. **Denial of service:**
   - The 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.



(d) Denial of service

## Security Services

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.

These services into five categories:

**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.

**Peer Entity Authentication**

Used in association with a logical connection to provide confidence in the identity of the entities connected.

**Data Origin Authentication**

In a connectionless transfer, provides assurance that the source of received data is as claimed.

**ACCESS CONTROL**

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

**DATA CONFIDENTIALITY**

The protection of data from unauthorized disclosure. 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.

**Connection Confidentiality**

The protection of all user data on a connection.

**Connectionless Confidentiality**

The protection of all user data in a single data block

**Selective-Field Confidentiality**

The confidentiality of selected fields within the user data on a connection or in a single data block.

**Traffic Flow Confidentiality**

The protection of the information that might be derived from observation of traffic flows.

**DATA INTEGRITY**

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

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.

**Connection Integrity with Recovery**

Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

**Connection Integrity without Recovery**

As above, but provides only detection without recovery.

**Selective-Field Connection Integrity**

Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

**Connectionless Integrity**

Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

**Selective-Field Connectionless Integrity**

Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

**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.

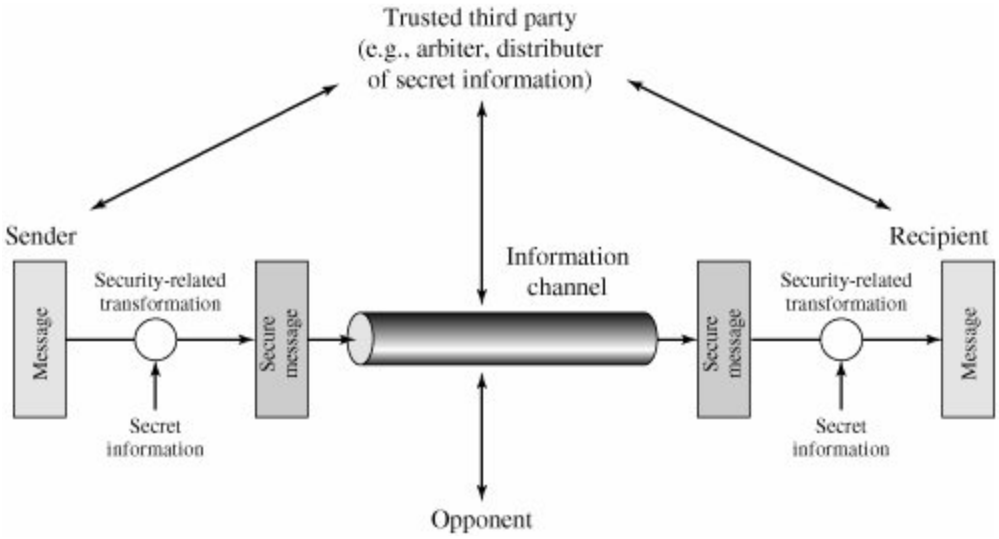
**Nonrepudiation, Origin**

Proof that the message was sent by the specified party.

**Nonrepudiation, Destination**

Proof that the message was received by the specified party.

## Model for Network Security




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.

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.