**Computer Security:**

**•** Computer security is the protection of computer systems and information from harm, theft, and unauthorized use.

**•** Generic name for the collection of tools designed to protect data and to thwart(prevent) hackers.

**Network Security :**

**•** Network security is any activity designed to protect the usability and integrity of your network and data.

**•** It measures to protect data during their transmission.

**•** This area covers the use of cryptographic algorithms in network protocols and network applications.

**•** Network Security consists of the provisions and policies adapted by network Administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

**Cryptography:**

**•** Cryptography is technique of securing information and communications through use of codes so that only sender and those person for whom the information is intended can understand it and process it.

**•** Thus preventing unauthorized access to information.

**•** The prefix “crypt”(Greek word: kryptos) means “hidden” and suffix “graphy” means “writing”.

**•** In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it.

**Terminology:**

**• Plaintext -** the original message

**• Cipher text -** the coded message

**• Cipher -** algorithm for transforming plain text to cipher text

**• Key -** info used in cipher known only to sender/receiver

**• Encipher (Encrypt) -** converting plain text to cipher text

**• Decipher (Decrypt) -** recovering cipher text from plaintext

**• Cryptography -** study of encryption principles/methods

**• Cryptanalysis (code breaking) -** the study of principles/ methods of deciphering cipher text without knowing key

**• Cryptology -** the field of both cryptography and cryptanalysis

**Security Goals**

The three security goals: confidentiality, integrity, and availability



**1. Confidentiality:**

* It is the most common aspect of information security. We need to protect our confidential information.
* An organization needs to guard against those malicious actions that endanger the confidentiality of its information.
* In the military, concealment of sensitive information is the major concern.
* In industry, hiding some information from competitors is crucial to the operation of the organization.
* In banking, customer’s accounts need to be kept secret.
* Confidentiality not only applies to the storage of the information, is also applies to the transmission of information.

**2. Integrity:**

* Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of her account needs to be changed.
* Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.
* Integrity violation is not necessarily the result of a malicious act: an interruption in the system, such as a power surge (up and down), may also create unwanted changes in some information.

**3. Availability:**

* The third component of information security is availability.
* The information created and stored by an organization needs to be available to authorized entities. Information is useless, if it is not available.
* The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity.

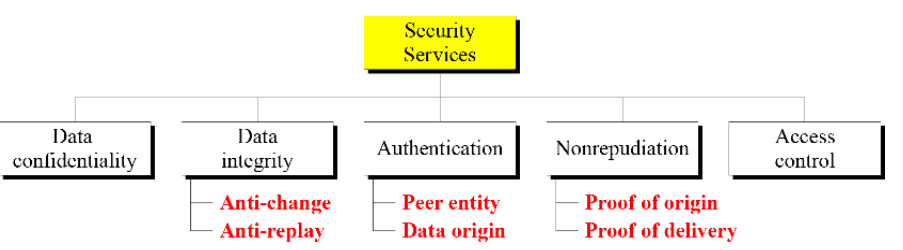
**Services and Mechanism**

* ITU-T (International Telecommunication Union-Telecommunication Standardization Sector)

provides some security services and some mechanisms to implement those services.

**Security Services**

* A service that enhances the security of data processing systems and information transfers.
* A security service makes use of one or more security mechanisms.
* ITU-T (X.800) has defined five services related to the security goals and attacks we defined in the previous sections.
* Figure shows the taxonomy of those five common services.



* It is easy to relate one or more of these services to one or more of the security goals.
* It is also easy to see that these services have been designed to prevent the security attacks that we have mentioned.

**1. Data Confidentiality:**

* Data confidentiality is designed for information is not made available to unauthorized individual.
* Confidentiality is the protection of transmitted data from passive attacks
* It is designed to prevent snooping and traffic analysis attacks.
* 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.

**2. Data Integrity:**

* Ensures that only authorized parties are able to modify computer system assets and transmitted information.
* It is designed to protect data from modification, changing status, insertion, deletion, and replaying by an adversary.
* It may protect the whole message or part of the message.

**3. Authentication:**

* The authentication service is concerned with assuring that a communication is Authentic.
* The assurance that the communicating entity is the one that it claims to be.
* Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
* This service provides the authentication of the party at the other end of the line.
* In connection oriented communication, it provides authentication of the sender and receiver during the connection establishment.
* In connection-less communication, it authenticates the source of the data (data origin authentication).

**4. Nonrepudiation:**

* Requires that neither the sender nor the receiver of a message be able to deny the transmission.
* 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 service protects against repudiation (refuse to accept) by either the sender or the receiver of the data.
  + **Nonrepudiation, Origin**

Proof that the message was sent by the specified party.

* + **Nonrepudiation, Destination**

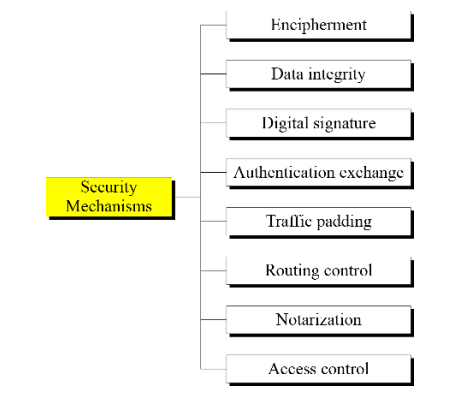
Proof that the message was received by the specified party.

**5. Access Control:**

* Requires that access to information resources may be controlled by the target system .
* Access control is the ability to limit and control the access to host systems and applications via communications links.
* It provides protection against unauthorized access to data.
* To achieve this, each entity trying to gain access must first be identified, or authenticated
* The term access in this definition is very broad and can involve reading, writing, modifying, executing programs, and so on.

**Security Mechanisms**

* A security mechanism is any process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
* ITU-T (X.800) also recommends some security mechanisms to provide the security services defined in the previous section.
* Figure gives the taxonomy of these mechanisms.



**1. Encipherment:**

* Encipherment, hiding or covering data, can provide confidentiality.
* Today two techniques cryptography and steganography are used or enciphering.

**2. Data integrity:**

* The data integrity mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself.
* The receiver receives the data and checks value.
* He creates a new checkvalue from the received data and compares the newly created checkvalue with the one received.
* If two check values are same, the integrity of data has been preserved.

**3. Digital signature:**

* A digital signature is a means by which the sender can electronically sign the data and receiver can electronically verify the signature.
* The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly.
* The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

**4. Authentication exchange:**

* In this two entities exchange some messages to prove their identity to each other.
* For example, one entity can prove that she knows a secret that only she is supposed to know

**5. Traffic Padding:**

* This means inserting some bogus data into the data traffic to the adversary's attempt to use the traffic analysis.

**6. Routing control:**

* It means selecting and continuously changing different available routes between sender and receiver to prevent the opponent from eavesdropping (secretly listen to a conversation) on a particular route.

**7. Notarization:**

* It means selecting a third trusted party to control the communication between two entities.
* This can be done, for example, to prevent repudiation.

**8. Access control:**

* It uses methods to prove that a user has access right to the data or resources owned by a system.
* Examples of proofs are passwords and PINs.

**SECURITY ATTACKS**

* Security attacks refer to the sets of actions that the threat actors perform to gain any unauthorised access, cause damage to systems/computers, steal data, or compromise the computer networks.
* An attacker can launch a cyber-attack from any location.
* The attacker can also be an individual or even a group.

security attacks can be of the following two types:

* Passive attacks
* Active attacks

**Passive Attacks**

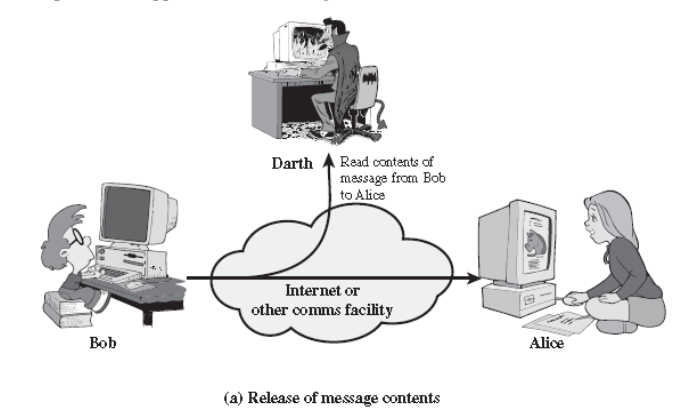
* A passive attack attempts to learn or make use of information from the system but does not affect or harm system resources.
* Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
* The goal of the opponent is to obtain information that is being transmitted.
* Two types of passive attacks are:

1. Release of message contents

2. Traffic analysis

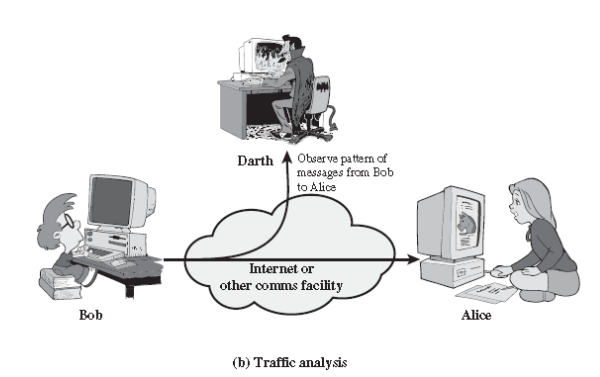
1. **Release of message contents:**

* 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.
* In this type of passive attack, the information transmitted from one person to another gets into the hands of a third person/hacker.
* It jeopardises the confidentiality factor in a conversation.



1. **Traffic analysis:**

* 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 attack:**

* An active attack attempts to alter or harm system resources or affect their operation.
* Active attacks involve some modification of the data stream or the creation of a false stream.
* Active attacks can be subdivided into four categories:

1. masquerade

2. replay

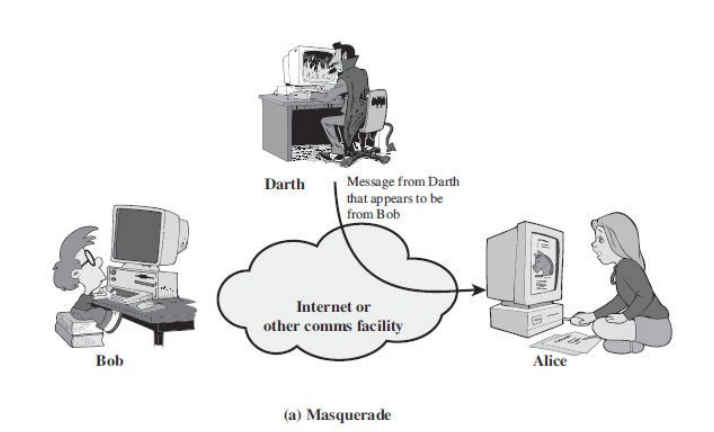
3. modification of messages

4. Denial of service

5.Repudiation

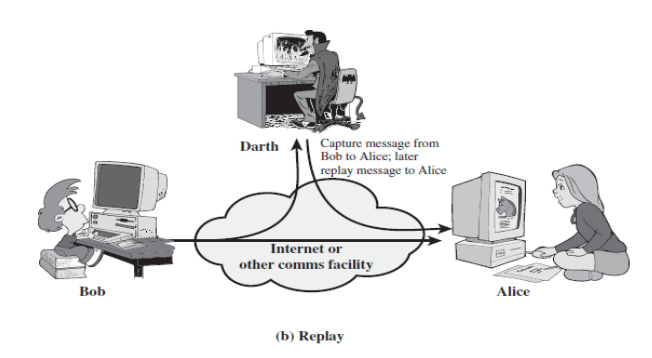
**1. Masquerade:**

* 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.



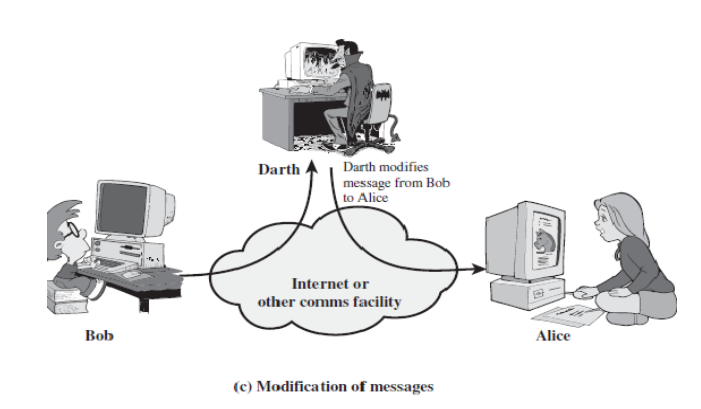
1. **Replay:**

* It involves the passive capture of a message and its subsequent transmission to produce an authorized effect.
* In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses.
* Once the data is corrupted or leaked it is insecure and unsafe for the users.
* For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive another payment from the bank.



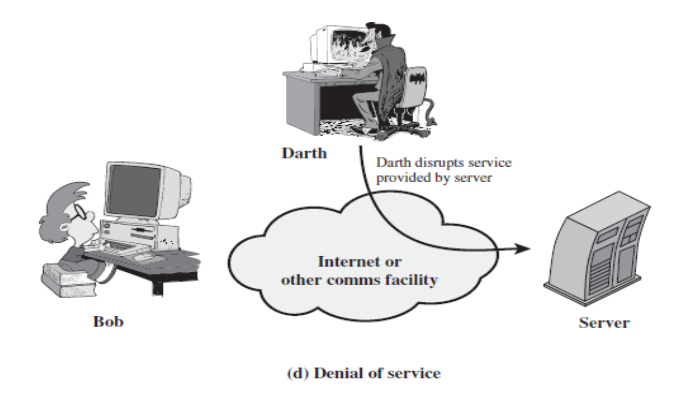
1. **Modification of messages:**

* 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 .
* 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”.
* Note that sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.



1. **Denial of service:**

* Denial of Service (DoS) is a very common attack.
* It may slow down or totally interrupt the service of a system.
* 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.

****

1. **Repudiation**

* Repudiation attacks are a type of cybersecurity attack in which an attacker attempts to deny or repudiate actions that they have taken, such as making a transaction or sending a message.
* These attacks can be a serious problem because they can make it difficult to track down the source of the attack or determine who is responsible for a particular action.

|  |  |  |
| --- | --- | --- |
| **On the basis of** | **Active attack** | **Passive attack** |
| **Definition** | In active attacks, the attacker intercepts the connection and efforts to modify the message's content. | In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes. |
| **Modification** | In an active attack, the attacker modifies the actual information. | In passive attacks, information remains unchanged. |
| **Victim** | In active attacks, the victim gets notified about the attack. | Unlike active attacks, in passive attacks, victims do not get informed about the attack. |
| **System's impact** | The damage done with active attacks can be harmful to the system and its resources. | The passive attacks do not harm the system. |
| **System resources** | In active attacks, the system resources can be changed. | In passive attacks, the system resources remain unchanged. |
| **Dangerous for** | They are dangerous for the integrity and availability of the message. | They can be dangerous for confidentiality of the message. |
| **Emphasis on** | In active attacks, attention is on detection. | In active attacks, attention is on prevention. |
| **Types** | Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service. | It involves traffic analysis, the release of a message. |
| **Prevention** | Active attacks are tough to restrict from entering systems or networks. | Unlike active attacks, passive attacks are easy to prohibit. |

| **Active Attack** | **Passive Attack** |
| --- | --- |
| In an active attack, Modification in information takes place. | While in a passive attack, Modification in the information does not take place. |
| Active Attack is a danger to **Integrity** as well as **availability**. | Passive Attack is a danger to **Confidentiality**. |
| In an active attack, attention is on prevention. | While in passive attack attention is on detection. |
| Due to active attacks, the execution system is always damaged. | While due to passive attack, there is no harm to the system. |
| In an active attack, Victim gets informed about the attack. | While in a passive attack, Victim does not get informed about the attack. |
| In an active attack, System resources can be changed. | While in passive attack, System resources are not changing. |
| Active attack influences the services of the system. | While in a passive attack, information and messages in the system or network are acquired. |
| In an active attack, information collected through passive attacks is used during execution. | While passive attacks are performed by collecting information such as passwords, and messages by themselves. |
| An active attack is tough to restrict from entering systems or networks. | Passive Attack is easy to prohibit in comparison to active attack. |
| Can be easily detected. | Very difficult to detect. |
| The purpose of an active attack is to harm the ecosystem. | The purpose of a passive attack is to learn about the ecosystem. |
| In an active attack, the original information is modified. | In passive attack original information is Unaffected. |
| The duration of an active attack is short. | The duration of a passive attack is long. |
| The prevention possibility of active attack is High | The prevention possibility of passive attack is low. |
| Complexity is High | Complexity is low. |