Introductions to Information Security

Information Security is the practice of securing information from unauthorized access. It is basically the method of preventing or reducing the impact of unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction, corruption of information. Information can be physical or electrical and tangible or intangible one.

Now in the era of information technology the Information Security is used in various fields like Cryptography, Mobile Computing, Cyber Forensics, On line Social Media etc.

➢ Information Security Parameters:

Information security's is primarily build on three objectives known as **CIA** triad these are Confidentiality, Integrity and Availability of data.

1. **Confidentiality:** Confidentiality of information means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.

2. **Integrity:** Integrity means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organization then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.

3. **Availability:** means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanding the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management.
   Denial of service attack is one of the factor that can hamper the availability of information.

Beside these, there are some others principals

4. **Non repudiation:** Non Repudiation means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example in cryptography it is sufficient to show that message

matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are per-requisites for Non repudiation.

5. **Authenticity:** means verifying that users are who they say they are and that each input arriving at destination is from a trusted source. This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission. For example if take above example sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches then it is known as valid transmission with the authentic or we say genuine message received at the recipient side.
6. **Accountability:** means that it should be possible to trace actions of an entity uniquely to that entity. For example as we discussed in Integrity section Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority for example Director of college and person that is allotted that change will be able to do change after verifying his bio metrics, thus timestamps with the user (doing changes) details get recorded. Thus we can say if a change goes like this then it will be possible to trace the actions uniquely to an entity.

- **Security violation**

1. Assumption, trust and Security assurance:

All the security policies and mechanisms rest on some assumptions. Policies which define security have to define correctly for a particular site. And all the mechanisms which enforce policies must also be appropriate. For a system it should ensure that we can trust all the transaction and transmission made by them.

Security assurance is a measure of how well and securely system meets its requirements, more formally how much we can trust the system to do what it is supposed to do. It covers how well the system does its job.

2. OSI security architecture.

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.

Security attack:

There are four general types of attacks,

Interruption

An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. e.g., destruction of piece of hardware, cutting of a communication line or disabling of file management system.

Interception

An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer. e.g., wire tapping to capture data in the network, illicit copying of files.

Modification

An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.

Fabrication

An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.

These Four types of attack can be categorically classified in two types

- **Active attack**

  An Active attack attempts to alter system resources or effect their operations. Active attack involves some modification of the data stream or creation of false statement. Types of active attacks are as following:

  Masquerade:
  Masquerade attack takes place when one entity pretends to be different

entity. A Masquerade attack involves one of the other forms of active attacks.

Modification of messages:
It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

Repudiation:
This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has sent or receive a message. For example, customer asks his Bank “To transfer an amount to someone” and later on the sender (customer) denies that he had made such a request. This is repudiation.

Replay:
It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.

Denial of Service:
It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network withers by disabling the network or by overloading it by messages so as to degrade performance.

- **Passive attack**

  A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

  The release of message content:
  Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

  Traffic analysis:
  Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
  The opponent could determine the location and identity of communicating host 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.

➢ Security mechanisms and Services

Security mechanism:

One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are:

Encipherment:

Encipherment ensures confidentiality by hiding or covering the data. Now two techniques are used to for encipherment,

Cryptography: Cryptography is the process of secrete writing to protect the date from attackers, that means the sender will not sent the original plain text, rather it convert the plain text to some cipher text by an encryption algorithm with secrete keys. And receiver after receiving the cipher text decrypts it with a decryption algorithm.

Steganography: In contrast to cryptography another popular method used as security mechanism is steganography. It means Covering of data. It does not alter the plaintext to another form; rather it hides the original data or file to another same or different type of file secretly. The text, audio, video, image or any other kind of file can be the medium of secrete data in steganography.

Data integrity:

We can ensure the integrity of data between transmissions by appends a short check value that is created by a specific process from the data itself. The receiver receives the data and creates a new check value from the received data. Comparing the check value created at receiver end with the value received we can check the integrity. If the two check values are the same the integrity of data has been preserved.

Digital Signature:

Digital signature is the mechanism to electronically sign the data before transmission and electronically verify the data at receiver end. Sender uses a process that involves a private key and a related public key which is publically known to all the receiver. The receiver uses the public key to prove that the massage is indeed signed by the sender who claims to have sent the massage.

Authentication exchange:

In this mechanism sender and receiver exchange some secrete massage to prove their identity to each other.

Traffic padding:

Traffic padding means inserting some random bogus data into the data stream, where data stream is not available. It is used to prevent traffic analysis and hide the traffic pattern from the attacker.

Routing Control:

Routing Control is the technique of selecting and changing the routes between sender and receiver to prevent the attack on a particular route.

Access Control:

Access Controls are the methods that ensure a user has access right to the data and resources owned by a system, these maybe Password or PIN Protection.

Notarization:

In notarization a third trusted party is used to control the communication between sender and receiver. As example for a transaction a third party can store the sender request in order to prevent the sender from later denying.

Security Services:

Data confidentiality:

Data Confidentiality is designed to protect data from disclosure to the attacker and protect the data stream from the attacker to analysis.

Data integrity:

This service is designed to protect data from modification, deletion, insertion or replying by the attacker.

Authentication:

This service provides the authentication of the parties to the other end of the transmission. It authenticates the receiver or sender during the establishment of a connection oriented communication and the source of the data in connection less communications.

Nonrepudiation:

It protects against repudiation by sender or receiver of the data. In non repudiation the receiver can proof the identity of the sender by the proof of origin if the sender denied later. And on the other side the sender can prove that data were delivered to the recipient with the proof of delivery.

Access Control:

This service provides protection against the unauthorized access to the data or resources on a particular system.

Relation between Security Services and Security Mechanisms:

The following table shows the relation between all the security services and the corresponding Security mechanisms used to achieve the security goals.

Security Service	Security Mechanism
Data confidentiality	Encipherments and Routing Control.
Data integrity	Encipherment, Digital Signature, Data integrity
Authentication	Encipherment, Digital signature, Authentication exchanges
Nonrepudiation	Digital Signature, Data integrity, and Notarization.
Access Control	Access Control Mechanism.

……………………..Continued