**COMPUTER SECURITY**

Computer security is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

**Security Goals (CIA triad)**

❖ **Confidentiality:**

It refers to the ability to hide the information from people who do not have the permission to access it. This helps to ensure that the data is not compromised to unauthorized people. Some of the method employed to ensure confidentiality is encryption & cryptography. For e.g. credit card transactions over the internet.

❖ **Integrity:**

It refers to the ability of protecting the data from modification or deletion by unauthorized people. Data integrity ensures that the data is the accurate and unmodified version of the original data.

❖ **Availability:**

Though it is highly necessary to ensure that the data is unavailable to unauthorized people, it is equally important to make sure that the data is available to authorized people. People who are authorized to access information must not face any issues when accessing information that is needed.

**Security Threat and Security Attack**

❖ **Security Threats:**

An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.Attacks are typically categorized based on the action performed by the attacker. An attack, thus, can be passive or active.

➔ *Passive Attack:*

◆ A passive attack make use of information from the system but doesn’t affect the system resources.

◆ The goal of attacker is to obtain the information that is being transmitted.

◆ Passive attacks are difficult to detect because they do not involve any alteration of data.

➔ *Active Attack:*

◆ These attacks attempts to alter system resources or affect their operations.

◆ It involves some modification of the data stream or creation of false stream.

**Security Services:**

A security service is something that enhances the security of data processing systems and 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 services.

● **Confidentiality:**

It is a security service that keeps the information secure from an unauthorized person. Encryption is a process to ensure the confidentiality.

● **Data integrity:**

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

● **Non-repudiation:**

Prevents either sender or receiver from denying message transmission or receipt of message.

Origin non-repudiation: preventing sender from denying that he has sent a message.

Destination non-repudiation: preventing receiver from denying that he has received a message.

● **Access control:**

The prevention of the 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).

● **Availability:**

Making system or resources available upon demand by legitimate users.

**Security Mechanism:**

Security mechanisms deal with prevention, detection, and recovery from a security attack. Prevention involves mechanisms to

prevent the computer from being damaged. Detection requires mechanisms that allow detection of when, how, and by whom

an attack occurred.

➔ **Cryptography:**

Cryptography is the science of writing information in a “hidden” or “secret” form and is an ancient art. Cryptography is necessary when communicating data over any network, particularly the Internet. It protects the data in transit and also the data stored on the disk.

➔ **Firewall:**

A firewall is a security mechanism to protect a local network from the threats it may face while interacting with other networks (Internet). A firewall can be a hardware component, a software component, or a combination of both. It prevents computers in one network domain from communicating directly with other network domains.

➔ **Users identification and authentication**

Identification is the ability to identify uniquely a user of a system or an application that is running in the system. Authentication is the ability to prove that a user or application is genuinely who that person or what that application claims to be.

➔ **Intrusion Detection System (IDS):**

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. There are two main types of IDS based on where the security team sets them up: Network intrusion detection system (NIDS). Host intrusion detection system (HIDS).