Assignment No. 1

Q.1) Explain CIA triad in detail.

→ The CIA Triad - Confidentiality, Integrity, and Availability - is a guiding model in information Security.

1) Confidentiality :- Who is authorized to use data?

- Data confidentiality.
- Assures that ~~pro~~ private or confidential information is not made available or disclosed to unauthorized individuals.
- Privacy :- Assures that individuals control or influence what information related to them may be collected & stored & by whom & to whom that information may be disclosed.

2) Integrity :- Is data good?

- Data integrity :- Assures that information (both Stored & in transmitted packets) & programs are changed only in a specified & authorized manner.
- System integrity :- Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

3) Availability :-

- Can access data whenever need it?
- Assures that system work promptly & service is not denied to authorized users.
- Availability means data are accessible when you need them. Availability of data is crucial to daily operations of our institution. Without access to our data, everything grinds to a halt, which is why medical & educational institutions like WashU are often targeted for ransomware attacks.

Q.2 Write short note on OSI security Architecture.

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

1). Security attack :-

- Any action that compromises the security of information owned by an organization.
- The security attacks can be categorized as:

1) passive Attack :-

- A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- Two types of passive attacks are the release of message contents and traffic analysis.

2) Active Attack :-

- An active attack attempts to alter system resources or affect their operation.
- It can be subdivided into four categories: Masquerade, replay, modification of messages, and denial of service.
- A masquerade takes place when one entity pretends to be different entity.

2) Security Services.

Security services refer to the different services available for maintaining the security & safety of an organization. They help in preventing any potential risks to security. Security services are divided into 5 types.

- Authentication :- It is the process of verifying the identity of a user or device in order to grant

or deny access to a system or device.

- Access control :- It involves the use of policies and procedures to determine who is allowed to access specific resources within a system.
- Data Confidentiality :-
  It is responsible for the protection of information from being accessed or disclosed to unauthorized parties.
- Data integrity :- It is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission.
- Non-repudiation :- It involves the use of techniques to create a verifiable record of the origin & transmission of a message, which can be used to prevent the sender from denying that they sent the message.

3) Security Mechanism.
The mechanism that is built to identify any breach of security or attack on the organization, is called a security mechanism.

- Some examples of Security mechanisms include.

i) Encipherment (Encryption) involves the use of algorithms to transform data into a form that can only be read by someone with the appropriate decryption key.

ii) Digital Signature :- It is Security mechanism that involves use of cryptographic techniques to unique identifier for digital document or message.

iii) Traffic padding.

iv) Routing control

Q.3 What is security Attacks & explain their types & sub-types in detail.

→ A security Attacks is an attempt by a person or entity to gain unauthorized access to disrupt or compromise the secure security of a system, network, or compromise the security of a system device. These are defined as the action that put at risk an organization's safety. They are further classified into 2 sub-types.

1) Passive Attack

- A passive attack attempts to learn or make use of information from the system but not affect system resources.
- Two types of passive attacks are the release of message contents & traffic analysis.
- The relase of message contents is easily understood. A telephone conversation, an electronic mail message.
- A 2nd 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 The common technique for masking contents is encryption

2) Active Attack

- An active attack attempts to alter system resources or affect their operation.
- It can be subdivided into four categories: masquerde replay, modification of messages, and denial of service.
- A masquerade takes place when one entity pretends

to be a different entity.

- Replay involves the passive capture of a data unit & 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.
- The denial of service prevents or inhibits the normal use or management of communications facilities.

Q.4) What is security services & explain their types in detail.

→ Security services are used for maintaining security. these security services can be implemented in various layes of the OSI model. Security services can be divided into 5 major categories.

1) Authentication :-
This is a very basic & easy service to implement. In authentication, the system (both sender & receiver) identifies the user first. only the user authorized to enter the system can use it. This can be done using basic password protection

2) Access control :-
In an organization, various levels of access to the system. For ex., in a company, a software engineer has limited access to the system as compared to the product manager & the product manager has limited access as compared to the CIO of the company.

3) Confidentiality:-
This is one of the three pillars of the security model CIA (confidentiality, Integrity & Availability) Confidentiality means that the data i.e. is shared between a sender & receiver should be confidential to them only. No third party should be able to read the data.

4) Integrity:-
This is the second pillar of the CIA. Here, integrity means that no third party should be able to modify the data i.e. is shared between the Sender & the receiver.

5) Non-repudation:- 5.
So, let us say that the Sender sent some data to the receiver & the receiver has received the data as well. Now the receiver refuses to accept that the data has been received. So, there should be a way to clarify & prove that the receiver has received the data. The same is the case otherwise. So, when there are means to identify this in the security model, it is called non-repudiation

Q.5) What is Security Mechanism & explain their types in detail.

→) The mechanism that is built to identify any breach of security or attack on the organization is called a security mechanism. Security Mechanisms are also responsible for protecting a system, network or device against unauthorized access.
Some examples of security Mechanisms include:

- Encipherment (Encryption)
It involves the use of algorithms to transform data into a form that can only be read by someone with the appropriate decryption key. Encryption can be used to protect data it is transmitted over a network, or to protect data when it is stored on a device.
- Digital signature
It is a security mechanism that involves the use of algorithms ~~to transf~~ cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity & integrity of the document or message.
- Traffic padding :-
It is a technique used to add extra data to a network traffic stream in an attempt to obscure the true content of the traffic & make it more difficult to analyze.
- Routing control :-
It allows the selection of specific physically secure routes for specific data transmission & enables routing changes, particularly when a gap in security is suspected.