What is Information Security? Discuss its three objectives.

Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of Information. Information can be physical or electronic one. Information can be anything like your details or we can say your Profile on social media, your data in mobile phone, your biometric etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.

During First World War, Multi-tier Classification System was developed keeping in mind sensitivity of Information. With the beginning of Second World War formal alignment of classification System was done. Alan Turing was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data.

Information Security programs are build around 3 objectives, commonly known as CIA-

1. Confidentiality:- 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:- means maintaining accuracy and completeness of data. This means data can't be edited in an unauthorized way. For example if an employee leaves an organisation them 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 outstanded 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.

Explain the need for Information Security.

The need for Information security is :-

1. Protecting the functionality of the organization:
The decision maker in organizations must set policy and operates their organization in compliance with the complex, shifting legislation, efficient and capable applications.

2. Enabling the safe operation of applications:
The organization is under immense pressure to acquire and operates integrated, efficient and capable applications. The morden organization needs to create an environment that safeguards application that serves as important elements of the infrastructure of the organization.

3. Protecting the data that the organization collect and use:

Data in the organization can be in two forms are either in rest or in motion, the motion of data signifies that data is currently used for processed by the system. The values of the data motivated that attackers to seal or corrupts the data. This is essential for the integrity and the values of the organization's data. Information security ensures the protection of both data in motion as well as data in rest.

4. Safeguarding technology assets in Organizations:
The Organization must add intrastate services based on the size and scope of the organization. Organizations growth could lead to the need for public key infrastructure, PKI an integrated system of the software, encryption methodologies. The information security mechanism used by large organizations is complex in comparison to a small organizations. The small organization generally prefers symmetric key encryption of data.

Explain Malware on the basis of Infection method.

Malware is a combination of 2 Terms - Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories: Infection Method and Malware Actions

Malware on the Basis of Infection Method are following :

1. Virus :- They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and them they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.

2. Worms :- Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference b/w virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.

Trojan:- The concept of Trojen is completely different from the viruses and worms. The name Trojan is derived from the 'Trojen Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.
Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.
They often provide backdoor gateway for malicious programs or malevalent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, Remote Access Trojans etc.

Bots:- can be seen as advanced from of worms.
They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad.
Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called Botnet.

Explain Malware on the basis of Actions.

Malware on the basis of Actions:

1. Adware - Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer's desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An Attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.

2. Spyware :- It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection. One of the most common example of spyware is KEYLOGGER. The Basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.

Ransomware :- It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or

wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.

4. Scareware:- It masquesades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.

5. Rootkits:- are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.

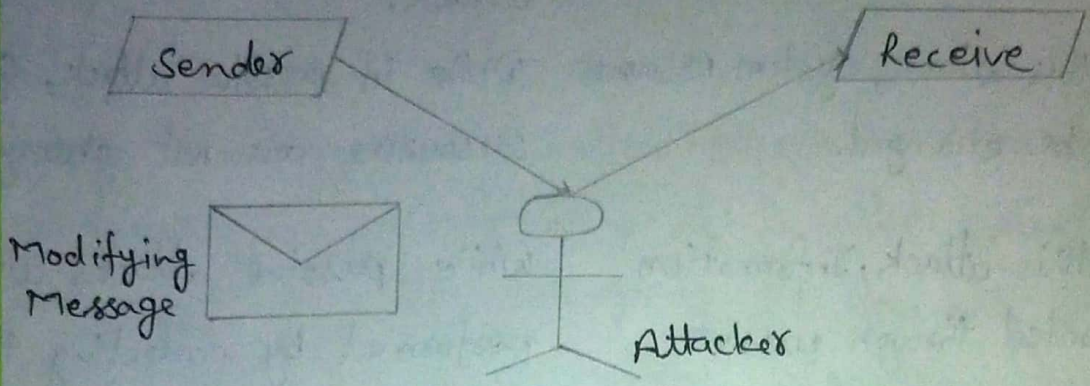
6. Zombies:- They work similar to spyware. Infection mechanism is same but they don't spy and steel information rather they wait for the command from hackers.

Differentiate Virus and Worms.

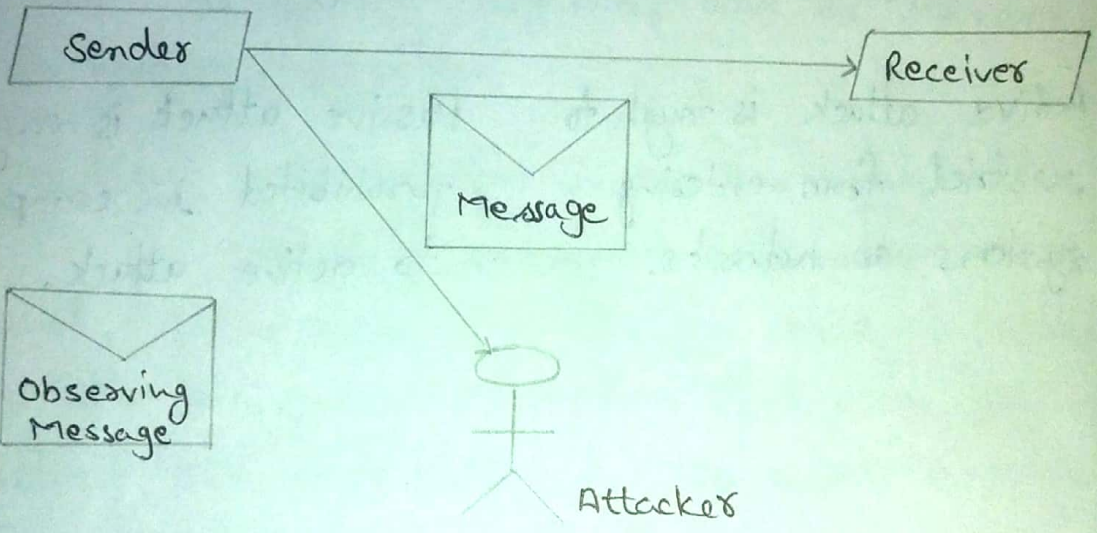
	Worms	Virus
1.	A worm is a form of malware that replicates itself and can spread to different computers via network.	A virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.
2.	The main objective of worm is to eat the system resources.	The main objective of viruses is to modify the information.
3.	It doesn't need a host to replicate from one computer to another.	It requires a host is needed for spreading.
4.	It is less harmful as compared.	It is more harmful.
5.	Worms can be controlled by remote.	Viruses can't be controlled by remote.
6.	Worms are executed via weaknesses in the system.	Viruses are executed via executable files.
7.	Example of worms include Morris worm, storm worm, etc.	Examples of viruses include Creeper, Blaster, Slammer, etc.

8.	Internet worms, Instant messaging worms, Emails worms, File sharing worms, Internet relay chat (IRC) worms are different types of worms.	Boot sector virus, Direct Action virus, Polymorphism virus, Macro virus, Overwrite virus, File Infector virus are different types of viruses.
9.	It does not need human action to replicate.	It needs human action to replicate.
10.	It spreading speed is faster.	It spreading speed is slower as compared.

Differentiate Active and Passive Attacks on Internet Security.



Active Attack



Passive Attack

Active Attack	Passive Attack
• In active attack Modification in information take place.	While in passive attack, Modification in the information does not take place.
• It is danger for Integrity as well as availability.	This is danger for Confidentiality.
• Due to this attack system is always damaged.	While due to passive attack, there is no any harm to the system.

• In active attack, Victim gets informed about the attack.	While in passive attack, Victim does not get informed about the attack.
• In this attack, System resources can be changed.	While in passive attack, System resources are not change.
• In this attack, Information collected through passive attacks are used during executing.	While passive attacks are performed by collecting the information such as passwords, message by itself.
• Active attack is tough to restrict from entering systems or networks.	Passive attack is easy to prohibited in comparison to active attack.

Define plain text, cipher text, encryption, decryption.

Plaintext and Ciphertext :-

The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm tranforms the plain text into ck ciphertext; a decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorith, and the receiver uses a decryption algorithm.

Decryption:- Decryption is the procedure of changing encrypted information into its original, decipherable format. The phase of decryption takes the ambiguous information that was originally received and interprets it into words and images that a human can understand.

Decryption is an important component of cybersecurity processes, because encryption needed scrambling words and pictures to securely send them to a multiple user through the Internet.

Encryption:- Encryption is a security approach where data is encoded and can only be accessed or decrypted by a user with the proper encryption key. Encrypted data is also called

a ciphertext. It can appears scrambled or illegible to a person or entity accessing without permission.

Encryption is an important method for individuals and organization to secure sensitive data from hacking. For instance, websites that transmit credit card and bank account numbers should continually encrypt this data to avoid identity theft and fraud. The numerical study and application of encryption is called a cryptography.

In encryption, it is based on the type of encryption, information can be shown as several numbers, letters, or symbols. Those who operate in cryptography fields create it their job, to encrypt data or to divide codes to receive encrypted information.

With the help of diagram explain a General Model for Network Security.

When we send our data from source side to destination side we have to use some transfer method like the internet or any other communication channel by which we are able to send our message. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. When the transfer of data happened from one source to another source some logical information channel is established b/w them 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.

When we use the protocol for this logical information channel the main aspect security has come. who may present a threat to confidentiality, authenticity, and so on. All the technique for providing security have to componets:

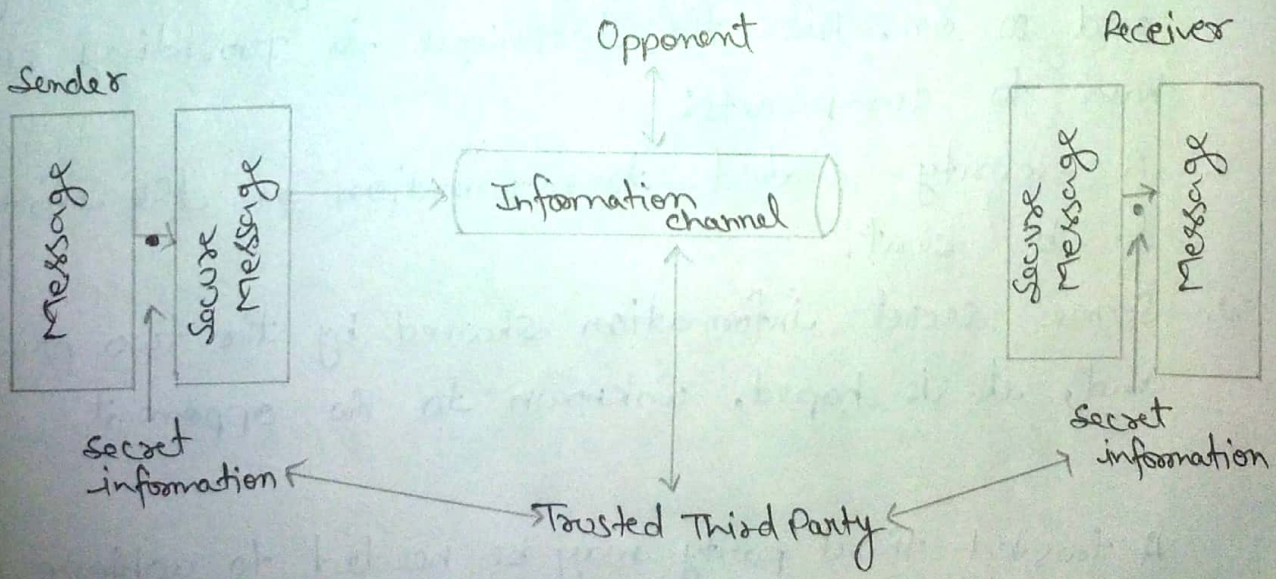
1. A security-related transformation on the information to be sent.
2. Some secret information shared by the two principal and, it is hoped, unknown to the opponent.

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 b/w the two principals concerning the authenticity of a message transmission.

This model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of secret information.
4. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service.



NETWORK SECURITY MODEL

How many vulnerabilities are there in Information security discuss each in details.

Vulnerabilities are weakness in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Even though the technologies are improving but the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weakness, etc. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.

1.) Hardware Vulnerability:

A hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely.
For examples:

a.) Old version of systems or devices
b.) Unprotected storage
c.) Unencrypted device, etc.

2.) Software Vulnerability:

A software error happen in development or configuration such as the execution of it can violate the security policy. For examples:

a.) Lack of input validation
b.) Cross-site scripting
c.) Unencrypted data, etc.
d.) Unverified uploads

3. Network Vulnerability:

A weakness happen in network which can be hardware or software. For examples:

a.) Unprotected communication
b.) Malware or malicious software (e.g.: Viruses, Keyloggers, Worms, etc)
c.) Social engineering attacks
d.) Misconfigured firewalls

4. Procedural Vulnerability:

A weakness happen in an organizational methods. For examples:

a) Password procedure - Password should follow the standard password policy.

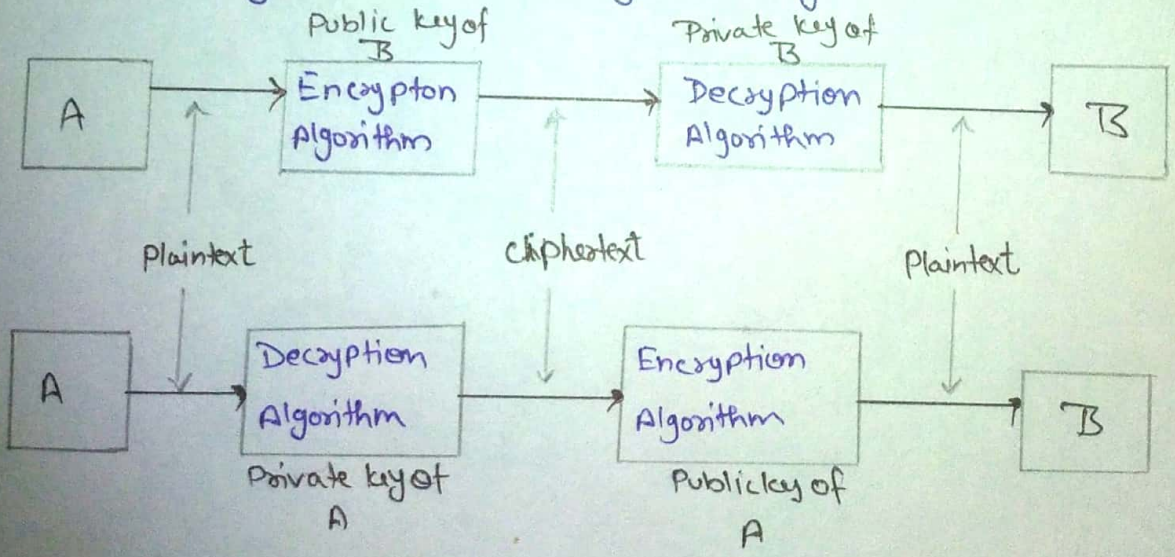
b) Training procedure - Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

Explain public key Encryption in detail.

Public key encryption algorithm is also called the Asymmetric algorithm. Asymmetric algorithms are those algorithms in which sender and receiver use different keys for encryption and decryption. Each sender is assigned a pair of keys:

- Public key
- Private key

The public key is used for encryption, and the Private key is used for decryption. Decryption cannot be done using a public key. The two keys are linked, but the private key cannot be derived from the public key. The public key is well known, but the private key is secret and it is known only the user who owns the key. It means that everybody can send a message to the user using user's public key. But only the user can decrypt the message using his Private key.



ENCRYPTION/DECRYPTION USING PUBLIC/PRIVATE KEYS

- The data to sent is encrypted by sender A using the public key of the intended receiver.
- B decrypts the received ciphertext using its private key, which is known only to B. B replies to A encrypting its message using A's public key.
- A decrypts the received ciphertext using its private key, which is known only to him.