Assignment no.1

M T W T F S S
Page No.:
Date: 07/10/22
YOUVA

Q.1) What is the need of security in computing environment?

→ • security refers to providing protection system to computer system resources such as CPU, memory, disk, software programs and most important data and information stored in the computer system.

• Needs of security in computing Environment:

a) Hardware and Software of the system needs to be secured from unauthorized access. Illegal use of processors, main memory and storage devices leads to loss of data Software need to be protected.

b) System needs to be secured from malicious programs like virus, worms.

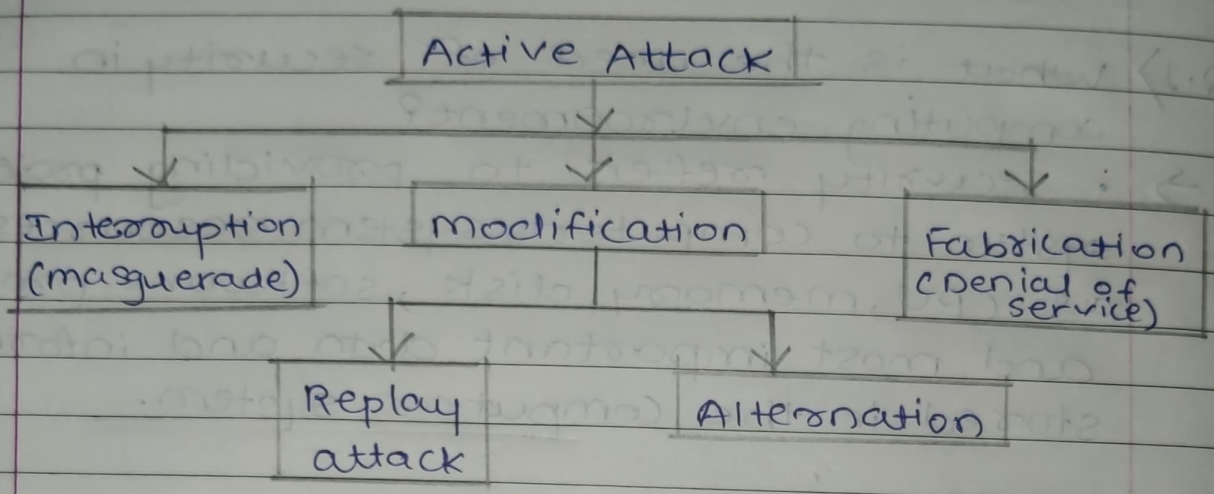
c) Unauthorized persons or attackers can crack the system security by hacking.

Q.2) Explain different types of security attacks.

→ • In a computer network there are two types of security attacks:-

a) Active attack.
b) Passive attack.

a) Active attack:-

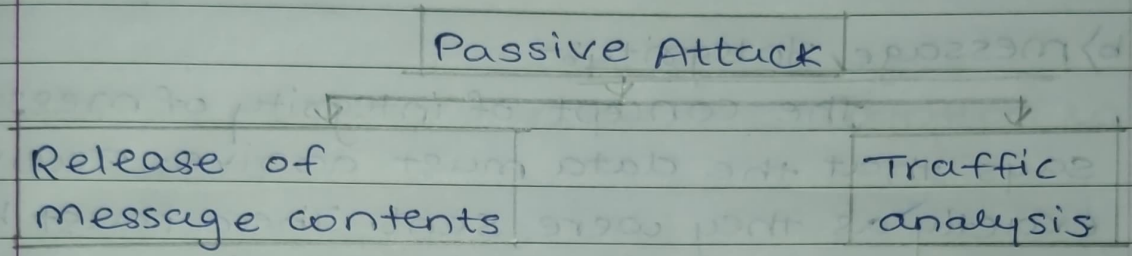


- Active attacks are based on modification of original message in same manner or the creation of false message.
- This attack cannot be prevented easily.
- They can be detected with some efforts & attempts can be made to recover from them.
- The contents of original message are modified in some ways.
- This attacks can be in the form of interruption, modification, fabrication.
- Interruption:- It is caused when unauthorise entity pretends to be another entity.
- Modification:- Modification attacks can be classified into Replay attack & alternation.

b) Passive attacks:-

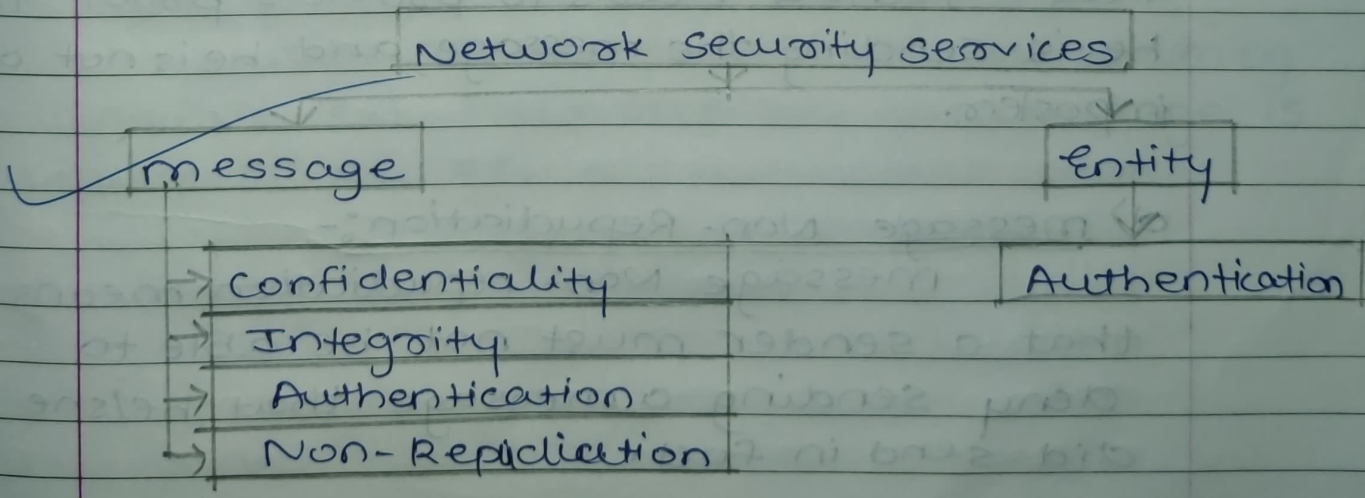
- Passive attacks are those where attacker is monitoring data transmission.
- The term Passive indicates that attackeros doesn't attempt to perform any modification to the data.

·This is also why passive attacks are harder to ~~deal~~ wi detect so the general approach to deal with passive attack is to think about prevention rather than detection or corrective action.



Q.3) Explain the network security services.

→ • Network security services means Confidentiality, Integrity, Authentication, Non-repudiation or Entity Authentication. These first four services are related to the message exchange using network while entity authentication service provides identification.



a) message confidentiality :-

The confidentiality make sense when the transmitted message must make

sense to only the expected receiver. The message must be garbage to all others. To achieve such privacy, sender must encrypt, encode the message and only receiver should decrypt, decode it.

b) **Message Integrity:-**

The concept of integrity of message says that the data must arrive receiver exactly as they were sent. There must be no alteration during transmission neither accidentally nor intentionally.

c) **Message Authentication:-**

Message Authentication ensures the receiver about sender's identity. It makes the receiver sure that an imposter hasn't sent the message. To provide authentication, sender needs to provide proof that he is sending the message and he is not an imposter.

d) **Message Non-Repudiation:-**

Message Non-repudiation means that a sender must not be able to deny sending a message that he/she did send in fact.

e) **Entity Authentication:-**

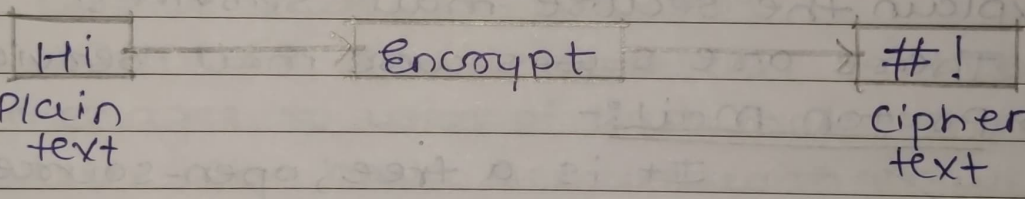
In this service of network security, entity or user is verified before accessing

the system resources. An entity can be a person, process, client or server. The entity whose identity needs to be verified is called 'CLAIMANT'. The party that tries to prove identity of CLAIMANT is called the 'VERIFIER'.

Q.4) Define Encryption and Decryption with diagram.

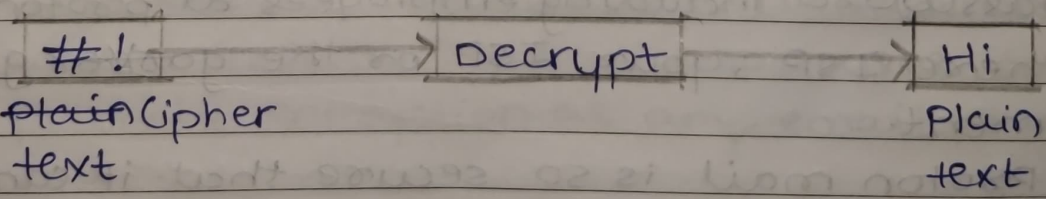
→ • **Encryption:-**

The process of encoding plain text messages into cipher text message is called as encryption.



• **Decryption:-**

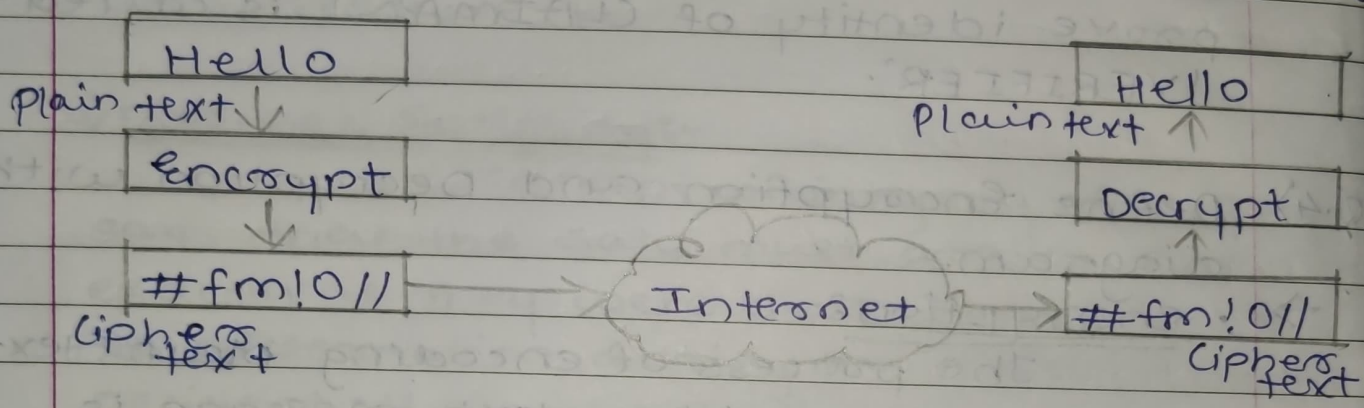
The reverse process of transforming cipher text back to plain text message is called as decryption.



• Every encryption and decryption process has two aspects:

a) The algorithm.
b) The key.

It makes the process of cryptography secured.



Q.5) Explain the secure mail services.

→ There are 5 secure mail services:-

a) Proton mail:-

- It is a free, open-source encrypted email provider. It works from any computer through website and also via android and iOS mobile apps.
- Nobody can decrypt your encrypted proton mail messages without your unique password including employees at proton mail, there ISP, your ISP or the ~~goo~~ government.
- Proton mail is so secure that it cannot recover your emails if you forgot your password.

b) Counter mail:-

- It offers a throughly secured implemen-

tation of open encrypted email in browsers.
- Only encrypted emails are stored on counters mail servers.
- This way decryption is impossible even if a hacker steals your password.
- It lets you modify lots of settings for your accounts. Forms can be built to send results to your email.

c) Hush email :-
- It is another encrypted email service that is being around since 1999.
- It keeps your email secured & locked behind state-of-the-art.
- With this service, you can send encrypted messages to users of Hush mail as well as non users who have account with gmail, outlook mail, or other similar email clients.

d) mailfence :-
- It is a security centric email service that features end-to-end encryption.
- The service includes email address and web interface that incorporates open publicly encryption as any email program have.
- You can create a key pair for your account and manage store of keys for people you want to mail securely.

e) Tutanota :-

- It is similar to proton mail in its design and security level.
- All tutanota emails are encrypted from sender to receiver and decrypted ~~at~~ right on the device.
- This email account is all you need to exchange secure ~~em~~ emails with other Tutanota users.
- For encrypted email outside system you specify a password for recepient to use when viewing the message in your browser that interface allows them to reply securely too.

Q.6) Explain different methods of protection.

→
- Application security. Secure coding. Secure by default.
- Computer access control. Authentication. Multi-factor authentication.
- Computer security software. Ativirus software.
- Data Centric Security.
- Code ~~of~~ obfuscation.
- Encryption.
- Firewall.
- Intrusion detection system. Host-based intrusion detection system (HIDS).

12/10/22