Unit-IV

Transport layer security:-

*It is refined in RFC 2246 (request for comments).
*TLS is needed for providing security in Transport layer.
*When the data is travelling from transport layer to next layer, we need to provide a security to the data.
*It is derived from SSL.
*It provides a secured connection blw client & server (i.e., no hacker (or) third party can interfrer in blw server and client).
*It is used by http, smtp.

Working:-

*It uses client server handshake mechanism. (ie., handshake blw the client and server).
*First, we have to establish the connection after that the key exchange blw client and server (By diffie hellman key exchange algorithm).
*once the key exchange is successful after TLS protocol will open an encryption channel (by RC4/IDEA/DES algorithm).
*It also ensures that the messages are not attered. It can be done by any of the hashing (↓charged) algorithm. like MD5/SHA Algorithm
*RFC 2246 is similar to SSL V3 (SSL version 3)

9] Web security Considerations:-

* whenever we are sending the data from one user to another user, always attacks will be there.
* In order to escape from the attacker we need security.
* security is required for websites.
* There are six security considerations:-
  1) updated softwares
  2) Beware of SQL injections
  3) cross site scripting (xss)
  4) Error message
  5] Data validation
  6] passwords.

1) updated software :-

* Let us you need always update your softwares. for example:- once you joining the office, if you wont to access the some of the office websites on your mobile, they will ask you that the phone should be updated time to time.

2] Beware of SQL injections:-

* SQL injections is nothing but that the data is inserting in tables (i.e., rows (or) columns).
* The hacker will inserting the data in the form of rows and columns to distrub the integrity of the data.

3] cross site scripting (xss):-

* It is also called as xss.
* Attacker will send site scripting to your website, like any data is related into the client.

Ex:- Forms.

4) Error Message:-

* when we are giving the password & username to the any website. sometimes we are forget the password. In that case we will get error message like your password and username is wrong.
* In that cases the attacker will not have clarity wheather the attacker will enter the wrong password (or) wrong username.

5] Data validation:-

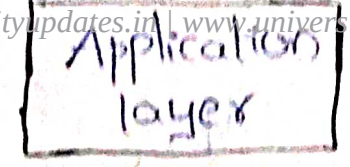
* Data validation should be done in both client side and server side.

6] passwords:-

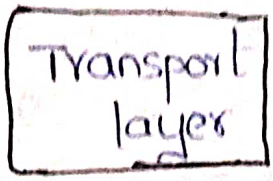
* The passwords are always should be strong (minimum 8 letters should be there).
* so, the attacker will not be able to get the password.

3] Secure Socket Layer:-

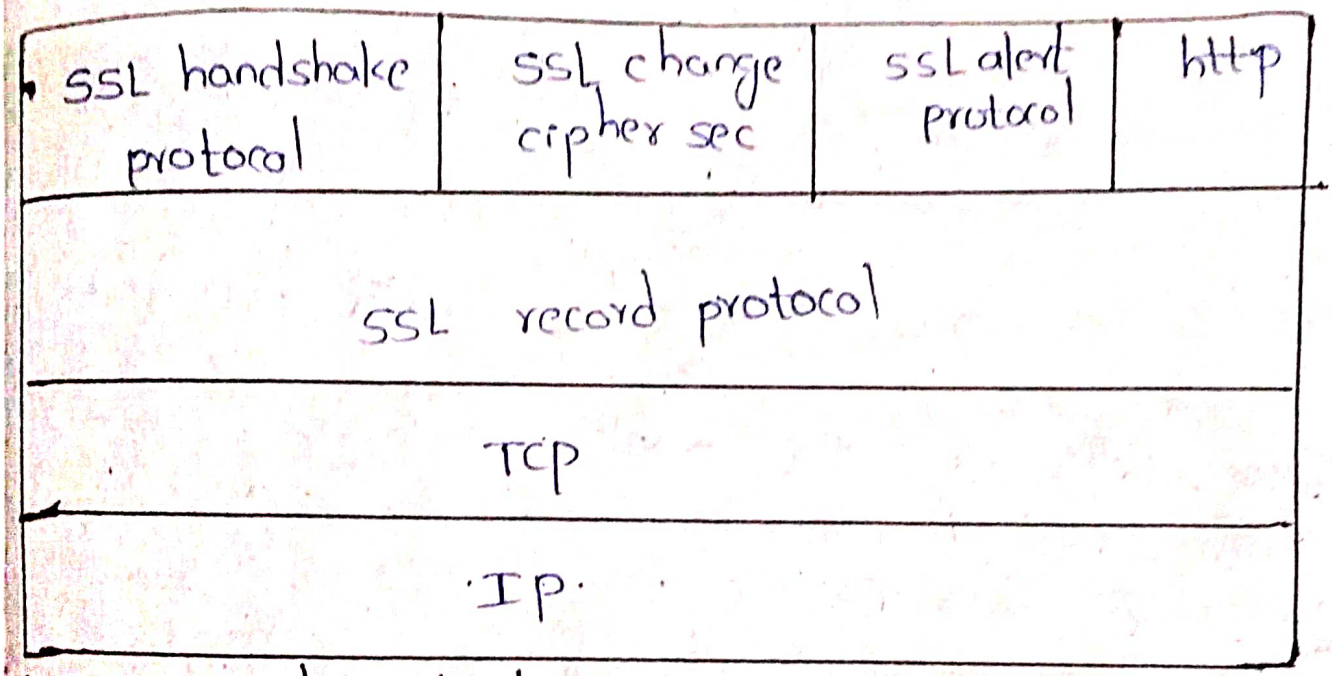
* It is used to provide security for communication blw two users.
* It ensures integrity, authentication and confidentiality.
* It lies blw application layer and transport layer of TCP/IP protocol.



→ SSL



* protocol stack of SSL:-

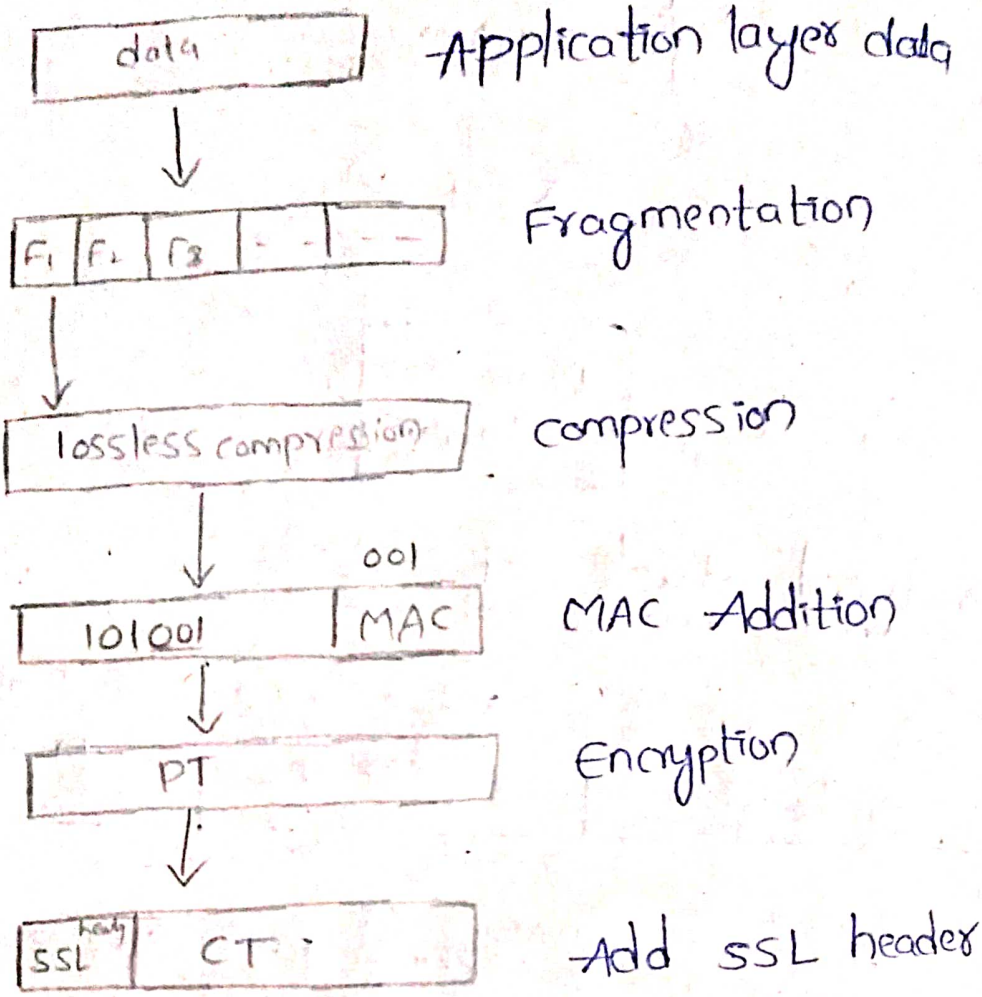


1) SSL record protocol:-

* It provides two services

1) confidentiality → by encryption
2) Message integrity → by MAC.

Working:-



* The data in the application layer is divided into no. of fragments based on the size of the data. This process is known as fragmentation
* The size of the each fragment is 2^{14} byte block.
* For each and every fragment there is a separate process.
* Take one fragment and do that data compression means you have to reduce the size of data.
* This compression has to be lossless compression
* Cale have to calculate the MAC code of the data and add this MAC code at the end of the data
* For the complete data block do the encryption.

* Encryption is done for to ensure the confidentiality.
* Before the encryption, the data can be called as plain text.
* After encryption, we will get the corresponding cipher text.
* We have to add SSL Header at the beginning of the cipher text.

SSL Handshake protocol:-

* SSL Handshake protocol is used to ensure Authentication
* Most complicated part in SSL
* It will do key exchange blw client and server.

Working:-

1. Connection establishment with server
2. key exchange from server to client } authentication
3. key exchange from client to server }
4. Handshake done from server.

SSL change cipher protocol:-

* It has only one message and size of the one message is 1 byte.
* It will copy the pending state into current state.

SSL Alert protocol:-

* whatever alerts related to SSL are sent to clients.
* Alerts is nthg but notifications.

*It has two bytes :- 1) Byte1 2) Byte2.

* Byte1 can have the value as ① or ②
value ① indicates the warning, if we ignore the warning then value ② becomes the fatal error. Then you need to stop it completely.

* Byte2 specifies the type of error.

HTTP:-

* Hypertext transfer protocol is an application layer protocol
* HTTP is a synchronous protocol, which in this case means that after a client sends a request to a server.
* It waits for a single response.
* The server can only respond to requests.

TCP:-

Transmission control protocol works with the internet protcol (IP) which defines how computers send packets of data to each other.

IP:-

* Internet protocol is the set of rules (ruling) governing the format of data sent via the internet (or) local network.

HTTPS (Hyper text transfer protocol secure):-

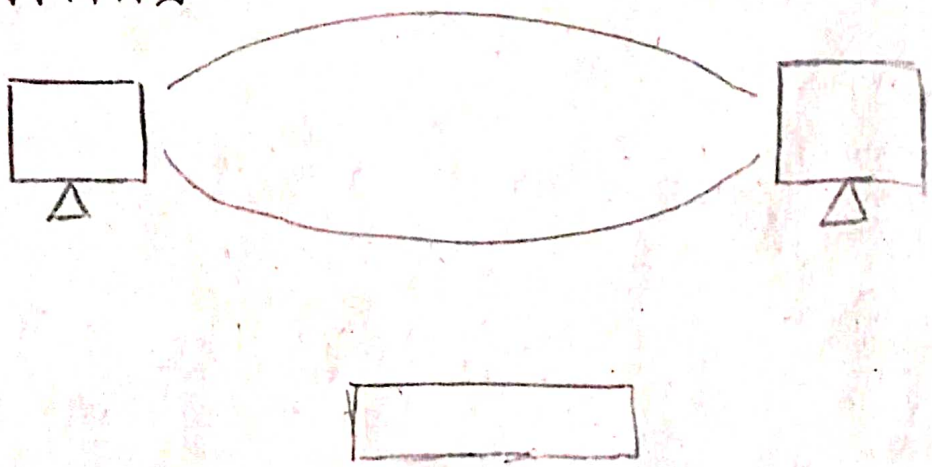
*It is a combination of http and ssL.
*It has an additional layer of security provided by TLS/ssL
* It is more secured compared to http
eg:- websites starting with (https://)
*In http data is in the form of plaintext only.
*In https data is in the form of plaintext and cipher text (i.e., encryption and decryption takes place).
*It belongs to transport layer protocol.
*It is heavier that http because it has an additional layer of security.
*It runs on port number 443 of server. and http runs on port number 80 of server
*It uses a certificate Authority (CA).
*it works on asymmetric key pkI and it uses ② different keys
1) private key:- It is avaliable on the web server and managed by owner of the server.
2) Public key:- It is avaliable to everyone (client and server can access)

* HTTPS is slower than http.
* The main usage of https are Banking websites, login credentials.

5] SSTL protocol (secure stlell):-

*It is a protocol for operating network service over an unsecured network.
*It is alternative to Telnet, FTP etc... (unsecured Protocols)
*It uses client server Architecture.
*It follows asymmetric key cryptography.
Two keys:- Encryption => public key
decryption => Private key.
*It provides confidentiality and Integrity.

Working:-



*client sends the request to the server.
*server will check the authentication of client with the public key.
*If public is matched then it will generate random string.
*The random string will send to the client, before sending to the client, the random string is encrypted and server sends the cipher text to

the client.

* The client will decrypt the cipher text with the help of private key.
* Again the decrypted data is sent back to the server.
* If client sent the correct decrypted data to the server, then server will believe that, the client is a trusted client.
* The authentication of client is conformed at the server side then SSTL Tunnel is created.
* SSTL Tunnel is a channel for communication blw client and server.
* No body can enter into the SSTL Tunnel to steal the data. means it is very secure.

PART-B

Wireless security:-

* protecting wireless n/w from unauthorised users

Ex:- Wifi, bluetooth etc...

* It is very complex in working.

factors contributing to risks in wireless n/w:-

- channel
- mobility
- Resources
- Accessibility.

*wireless n/w Threats:-

1) Malicious Association:- A wireless devices is configured in such a way that, to the user it will appears as a trusted device. But actually it is not a trusted device.

* The user will connect to it and all the data will be stolen by third party.

2) Adhoc network:-

* It is a wireless device which is not having the common access point (x) to communicate.

* For security purpose there is no chance.

3) Non-Traditional network:-

It is nothing but bluetooth, barcode, PDAs

* These are the wireless networks, so don't have much security.

4) Identity Theft:-

* For everything there is need of identity. that means everything have a unique barcode.

* The attacker will observe the network traffic, he will steal (or) findout the MAC address of the computer.

5) network injection:-

* Without the user notice, the data will be injected and this network injection mainly happens in the systems are exposed to non filtered network traffic.

Measures for wireless security:-

1. signal hiding techniques.
2. Encryption and authentication protocols.
3. use antivirus slw and firewalls
4. change Routers pre-set password
5. Allow only specific computers to access to your wireless nlw