UNIT-III

→ MD5 (Message Digest - 5)

Digest means dividing (or) breaking the bits (or) blocks

→ It is developed by Rivest.

→ It is fast and produces 128 bit Message.

→ Working of MD5:-

(1) Padding:- Padding means adding extra bits at end.

original msg + adding extra bits at end

→ If we add extra bits at the end the length should be 64 bit less than exact multiple of 512.

Ex:- Original msg = (1000 bits) + Padding

× 512 x 1 = 512 bits

× 512 x 2 = 1024 bits

✓ 513 x 3 = 1536 bits.

1536
- 64
1472 → it is total length.

Why, we are taking 1536 bits means it should be thousand and we should subtract 64 bits from 1536 bits. Because it should be multiple of 512.

1000 bits + 472 bits = 1472 bits

Here, we are adding (Padding) 472 bits

Scanned with CamScanner

2. Appending:- append the original length before padding

Here calculate length mod 64

→ In this most of the cases, 64 bits is obtained as answer

(∴ append 64 bits)

Ex: 1000 mod 64, Here we are adding 64 bits.

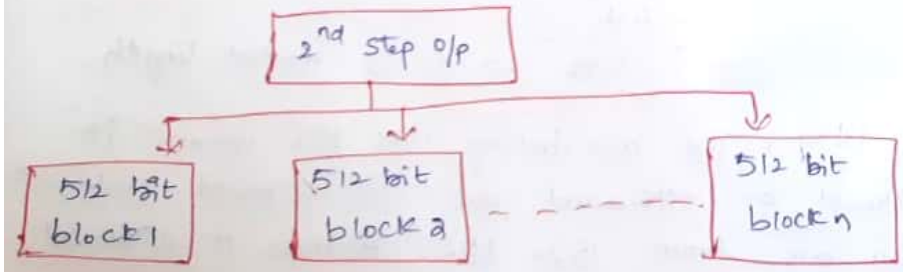
So, it again becomes multiple of 512.

3. Dividing:- Based on the length of the Output this is divided into Sub blocks.

Ex: 1. 1024 bits It is divided into 2 blocks

2. 1536 bits It is divided into 3 blocks.

→ Based on the output of 2nd step the blocks are divided.



4. Initialising:-

Initialise the variables.

(4 chaining variables).

of the length of the each & every [illegible]

32 bit.

A, B, C and D. Of these 4 values are predefined values itself.

5. Processing:-

In this 512 bit blocks are Processed.

1. Copy 4 chaining variables into some Corresponding variables.

A = a, B = b, C = c D = d

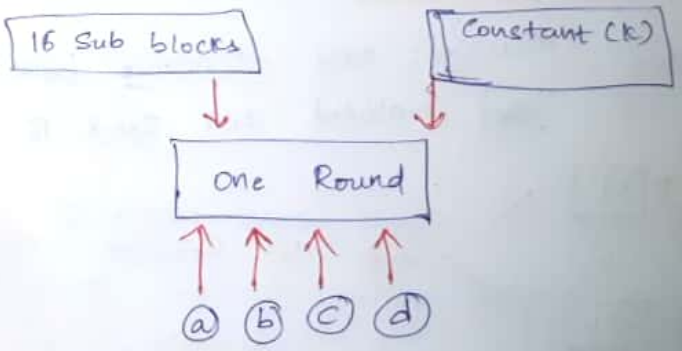
2. Divide 512 bit blocks into 16 - 32 bit blocks.

16 blocks and each of size 32 bits.

16 × 32 = 512

3. Four Rounds:-

16 Sub blocks and a Constant (k)



a = b + ((a + Process, P (b,c,d) + m[i] + T[k]))

b = a + ((b + Process, P (a,c,d) + m[i] + T[k]))

Scanned with CamScanner

We are having H variables, then we perform H rounds.

· Message digest means in this message is divided into sub blocks.

Message Authentication Code (MAC):-

→ It is similar to message digest.

→ In this Symmetric Key Cryptography is used.

Working of MAC:

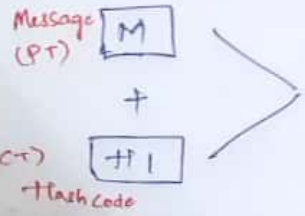
Senderside M ↓ ← Symmetric Key(K) → H1(MAC code)

If Sender wants to send a message 'm'

M(Hi, Hello) + Symmetric Key (K) = H1(MAC) is generated.

H1 → MAC mode → It is Cipher Text.

Now, Message and Hash code both are Combined and Send to receiver.



Receiver will calculate his own MAC (H2) by using Key (K); Key (K) means where the Key is same that we Sended from Sender side. Since it is symmetric we use same Key.

Here, H1, & H2 are generated.

Now, on Receiver Side, H1 & H2 are Compared.

H1 = H2 ⇒ If You sends 'Hi' msg to your friend if the same it is sent there is no change in msg.

H1 ≠ H2 If "H1" is not equal to "H2" the msg is changed that means in the middle the attacker came & changed the msg.

Significance of MAC:-

→ Receiver can know if message is changed.

→ Receiver has assurance that message is from correct Sender

(because same key for Sendur and Receiver)

HMAC & CMAC

HMAC: (HASH BASED MAC)

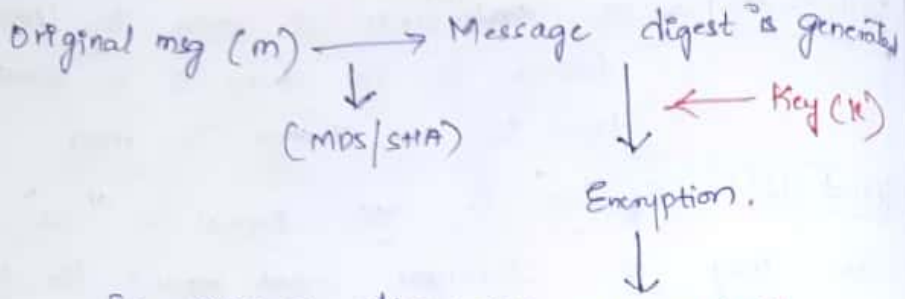
↳ H is used in Secure Socket Layer (SSL).

Working of (HMAC):

↳ Original msg (M) is Sended from Sender to Receiver by using either MD5/SHA algorithm You have to generate Message digest.

Scanned with CamScanner

Once you divide msg into sub blocks with the help of Key (K) we do Encryption. We Encrypt the original msg and we get CT. That CT is known as MAC.



In MAC → direct MAC is generated.

In HMAC → MAC is generated with help of msg digest.

CMAC:- According to our convenience we use MD5 (or) SHA Algorithm.

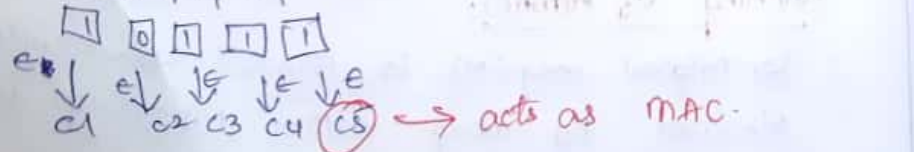
CMAC (CIPHER BASED MAC)

↳ It has size limit.

↳ It is based on block ciphers.

↳ Dividing msg into equal no. of blocks & each block is Encrypted separately.

Ex: 1011 1 → original msg (m)



→ acts as MAC.

Each & every block Encrypted separately

*Among all CT (multiple), last CT will

In Theoretical form:

$C_1 = E(K_1, A_1)$

$C_2 = E(K_1, (A_2 \oplus C_1))$

$C_3 = E(K_1, (A_3 \oplus C_2))$

$C_n = E(K_1, (A_n \oplus C_{n-1}))$

↓

This acts as MAC.

For Encrypt^n we take 2 i/p's: msg & key.

SHA-512

↳ SECURE HASH Algorithm

This algorithm is based on output bits.

The size of plaintext block → 1024 bits.

↳ Each block size is 1024 bits.

↳ No. of rounds − 80

↳ To perform different operations each round will produce a 64 word (w) → 64 bits

↳ We are generating w from PT.

↳ On each round we are using a constant K − Constant is in Hexadecimal.

↳ We use Buffers → the main purpose of Buffer is to store the intermediate results & to

Scanned with CamScanner

Output.

↳ Output of One Block is i/p to next block.
Each buffers size is 64 bits

↳ 8 Buffers are used in our Algorithm
(a, b, c, d, e, f, g, h)

Procedure:-

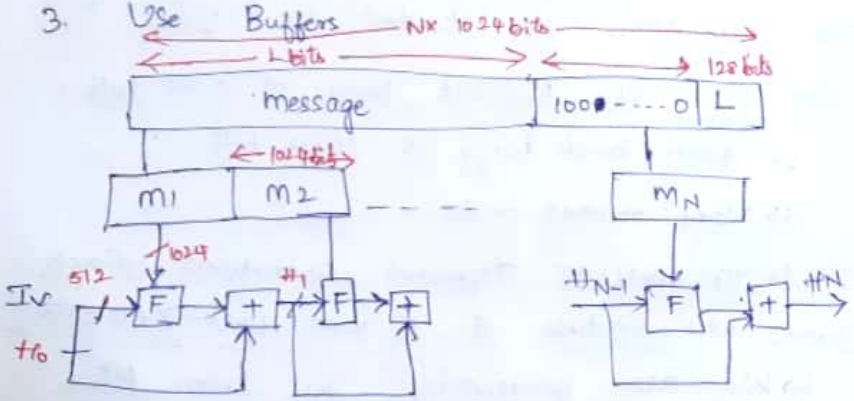
1. Padding

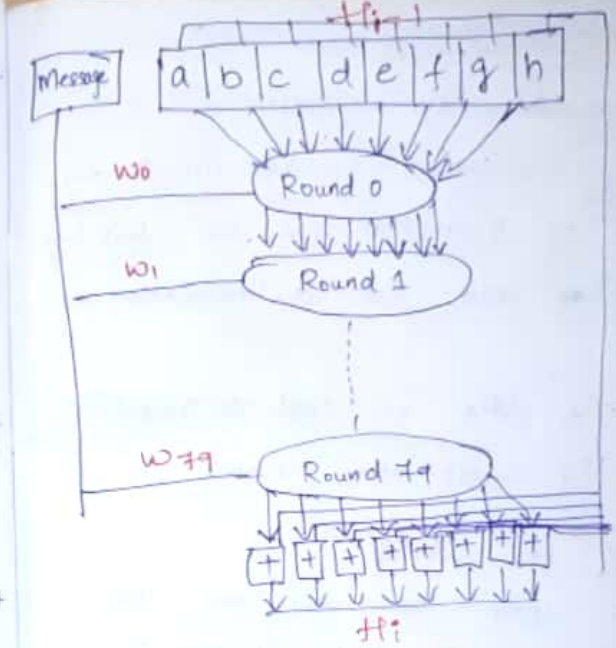
Taking the i/p, the ~~size~~ Size ~~Of~~ each block is 1024 bits

~~For Exe My PT Size is 1025~~

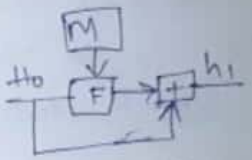
~~1 block 1024~~

1. Pad bits 1000 .... It is multiple of 1024 < 128
2. add 128 bits P.T at the end.
3. Use Buffers

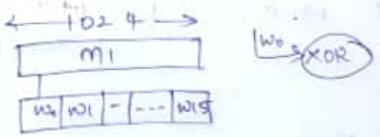




SHA Block Diagram



How words are generated from PT means:



Scanned with CamScanner

Digital Signature:-

→ It is Assymmetric key cryptography

→ In case of Encryption we use private key ie → In case of Decryption we use public key.

→ This is used in both for authentication and Non-Repudiation

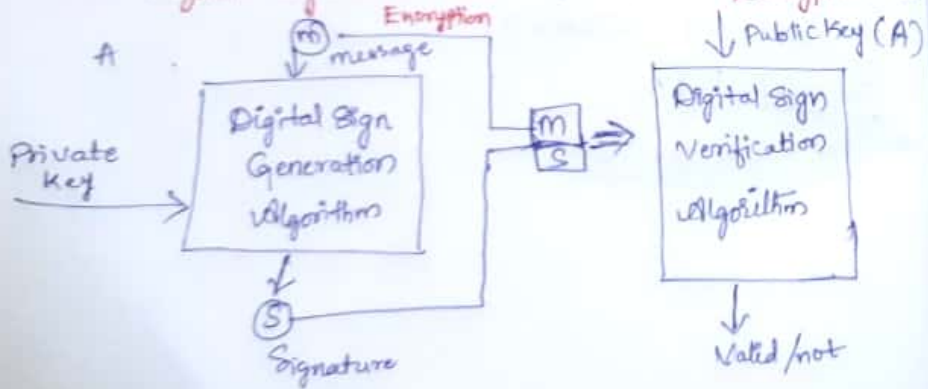
Authentication:- The data will sent to correct Person.

Non Repudiation:- You cannot deny the msg.

Signature:- Proof of Identity.

↳ If we apply for any card we must sign. Because, it is for identity, if it is in database, what you are details are correct or not. (Is it from correct sender/not)

How digital signature will work?



Both msg & Signature will send to Receiver

→ In encryption i/p is msg(m) & private key & o/p is msg & signature

↳ In Decryption, The receiver will use the public key of 'A' & the combined msg & he will verify this with the help of Digital Signature Verification Algorithm what will be the output for this Algorithm whether it is valid/not. (Initial msg 'm')

→ If msg is matched, it is valid.

→ If msg is not matched it is not valid.

* Key Management and Distribution.

* Key Distribution :(IN SYMMETRIC KEY)

There are 4 ways.

1. Physical delivery:- Sender and Receiver meet physically and exchanging the key. It is most Secured way. There is no loss of key for third person Because sender is meeting receiver directly.

Disadvantage:

↳ It takes more time.

~~How~~ ~~Means~~ Because, travelling time, waiting time is more.

2. Key distribution Center (KDC):- It will generate the key and it sends the key to both sender and Receiver

↳ It is takes less time.

↳ It is authenticate. Here, You have to rely on 3rd party. You have to depend on Key Distribution Center (KDC).

Scanned with CamScanner

3. Using Previous Keys:- Here we don't use old keys for encryption and Decryption. We generate new keys from old keys. Using previous old keys we will be generating new keys & and then you will be using new keys then, we will generate new keys by encrypting the old keys.

4. Using Third party:- First, 'A' is the sender, 'B' is the receiver in between there is 'c'. First A will send key to 'C' and then 'c' will send key to 'B'. So, that A & B will communicate through each other. But directly, A is not sending key to 'B'. this is all about key distribution in Symmetric Key.

*Key Distribution in Asymetric Key:-

there are 4 ways — Public key cryptography (2 keys)

1. Public Announcement:- Suppose we have a User 'A', this user 'A' will send its key to all (means it will broadcast key) to all users in networks. Particular Network Whoever user (B, C, D) wants the key they take the key of A & they do encryption and Decryption. Particular User will anounce the key to all the Users present in the network. (they will) This is simply Broadcasting.

2. Public Key directory (telephone directory):

we will have public key directory. All users will put there keys in public key directory. Suppose User B wants the key of User R. then User B will go to Public key directory he can search for 'R' he can take the key. Ex: how we search for Telephone no in Telephone directory that way User can come and search and take the required key. In Public key Directory we store the keys. If any modification or any adding new keys or update the keys that changes reflact in Public key directory.

3. Public Key Authority:- We have a trusted third party. All the user in n/w will depend on particular 3rd party. Suppose if A, wants to take the key of user 'B', then what happens means 'A' should send the request to this authority. Then the authority will send the public key of B to 'A'. Then it will check whether the user 'A' will belong to our n/w or not. User is 'A' is hacker or not. After checking it gives the public key of B.

4. Certificate Authority:- It is also similar to Public key Authority. It is also having a trusted Third party. The trusted third party is having all the users certificate who are in the n/w. The certificate will have the IP of the

Scanned with CamScanner

and public key. How the users will exchange the public key means they will check the Certificate of the users and they will take the public key.

* KERBEROS:-

→ It is a n/w authEntical protocol that if you want to use a particular services of a particular n/w that will provide if you are certified user. It will check whether the user is authenticated user or not. If yes it allows to the n/w.

→ It follows Client Server Architecture.

→ It follows Symmetric Key Algorithm.

→ In order to provide the keys it requires the Trusted Third party. (KDC) → Key Distribution Center. It provides database of all the secret keys.

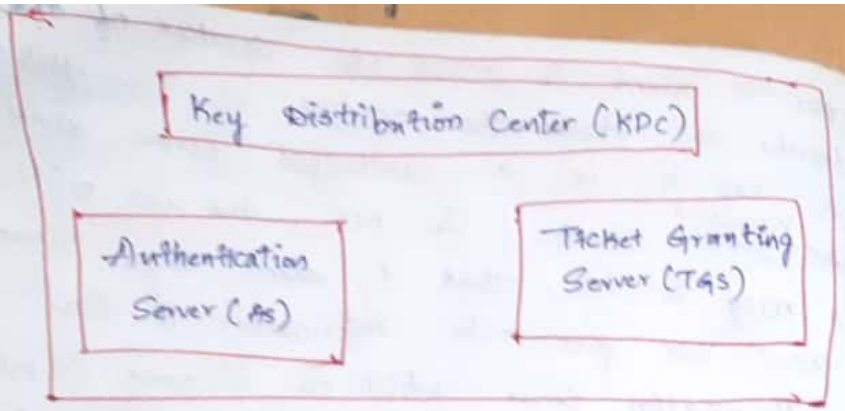
Working:- In Key distribution Center (KDC) there is having 2 Basic things. They are:

1. Authentication Server (AS)
2. Ticket Granting Server (TGS)

Every Key distribution Center is having 2 servers.

→ User A want to access the services of the n/w. Inorder to access the services of n/w the user has to be a authorized person and KDC (Kereberos will) check. In KDC, the user will send a msg to KDC, that I want keys. Then, KDC will give the information to the Authentication Server which is present in KDC will respond and send ticket to 'A'. So, this Ticket will be in encrypted format. The user has to perform the action on this Ticket. Inorder to understand what is present in that. The user will decrypt the msg. Then he will get hash code. The hash code again sent back to Authenticaticn server. Because it will check the Authenticity. If the user is able to decrypt it means he is certified user the server will known. It gives the Service Ticket (Inorder to access the Services) this services ticket is given to the Ticket Granting Server. This TGS will give Service Ticket to the User. Service Ticket is nothing but Secret Key. By using this Secret Key the user will Communicate with the n/w.

Scanned with CamScanner



User A

(Client)

Network Services

(Server)

X-509 AUTHENTICATION SERVICE :-

→ It is digital Certificate and this accepted internationally.

→ It does not generate any keys.

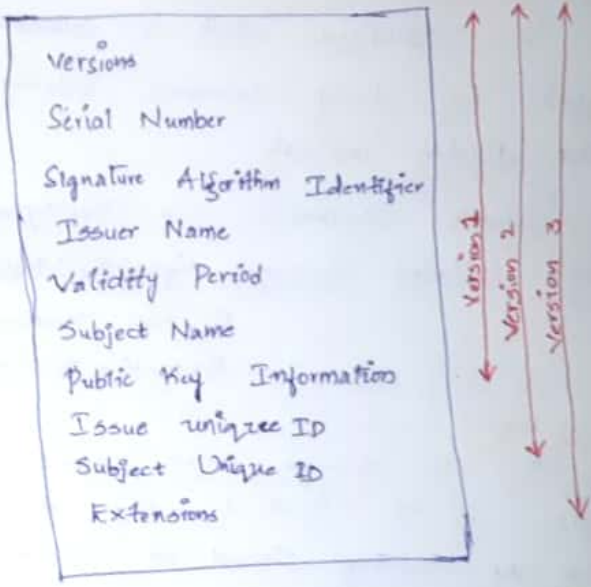
→ But it provides a way to access public keys.

→ It provides a Certificate stating that he is authorized user and certified user using that access you provide the keys. It provide you a way to access the key.

In X 509 Certificate also there are some Elements included.

It has 3 versions

Version:- Version means 1, 2, 3 Versions are there.



Signature Algorithm Identifier:- The person (Issuer) who is signing on the certificate. So, In order to sign the certificate who algorithm did the user will use it is present in signature Algorithm Identifier.

In certificate how the data will be present same in x.509 also certificate will be same.

Public Key Information: To encrypt or decrypt the public key is used means the subject the user is present in public key Information.

Scanned with CamScanner

Public Key Infrastructure (PKI):-

→ PKI is standard which is followed for digital Certificate. For doing managing, storing and revoking the digital Certificate.

→ It follows Assymmetric Key Cryptography.

→ It includes message digests, (Integrity)
Digital Signatures
Encryption Services (Confidentiality)

Msg Digest:

→ Why we use message Digest means for (Integrity) Purpose, If we send a msg it should reach same way nothing should be modified that is Integrity of the msg.

→ **Digital Signatures**: Why do we need digital Signature for authentication of msg. Ensuring that the msg has come from proper Sender or not.

→ If a sender sends msg to Receiver the receiver Cannot deny the msg is known as Non-Repudiation.

Encryption Services:- Inorder to Ensure the Confidentiality of the msg.

This is the Public Key Infrastructure.

Architecture Of Public Key Infrastructure (PKI):-

We have 4 parts.

1. Certificate Repository
2. Entity
3. Registration Authority (RA)
4. Certification Authority (CA)

1) **Certificate Repository:-** In general, repository means we store something. This is used to store all the Certificates and information related to all the certificate store in the Certificate Repository.

2) **Entity:-** Entity is nothing but it is the Users Of PKI. Who is using this. It is called Entity. It can be single person, Organisation, Router it can be anything the group of people whoever is trying to access the PKI that Entity is called as Entity.

3) **Registration Authority:-** (RA) It is for Registration and verification puapose. If anybody are raises the request for accessing the digital Certificate. then it will register the request. Whether the user must be trusted one.

4) **Certification Authority:-** (CA) CA will decide that whether we have to give certificate to the User or not. and also decides upto what limit I have to give.

Once registration is done it gives to the Certification Authority.

Scanned with CamScanner

UNIT - IV

Transport - level Security

Web Security Considerations:-

→ Why do we need Security for our websites
→ how can we Secure.

→ Whenever you are using the Internet (or) Clicking on any link (or) Sending when sending the data from Sender to receives we have vulnerabilities. Vulnerabilities means attackers will be there. In order to Escape from attacker we must have Security. Security is required for all the websites. Why do we need Security means inorder to protect the website from hackers.

∴ Security is required for websites.

Security Considerations:- How we can secure of Website. means there are 6 ways. They are:

1. **Updated softwares:-** We need to update the software. If there are any vulnerabilities (or) virus you can safeguard our website. If we update our software.

2. **Beware of SQL injections:-** SQL injections means the hackers will insert a row, or insert a column. SQL means mostly the data will be stored in tables. the hackers will Enter into the table and they disturb the rows & Columns by inserting the data. The integrity of data is disturbed. Any modification is done.

3. **Cross site Scripting(XSS):-** Attacker will send the Cross Scripting Client scripting into your website. any related details related to client like that he will send and he will hack.

For Ex: We can take forms. In forms faulty data is injected into through forms. Like we will have google forms there we submit our data in forms. that data will store in database and through that database the user will server will connecting back to you. The hacker will disturb the database, or he can correct the database, or by submitting multiple forms then the server database will get Over-flow. It effects the system.

4. **Error Message:-** Whenever you are giving User name and password for the any of the website some times when we forgot our password when we enter wrong password. We get error msg that your username/password is wrong.

Scanned with CamScanner

5. Data validation:- Data validation should be done Client Side and Server Side. Data validation means when the clients enters username and password, on the that data validation Server Side. On both sides the data validation should be done.

6. Passwords:- We should use strong passwords. Minimum Characters, Symbols will be there.

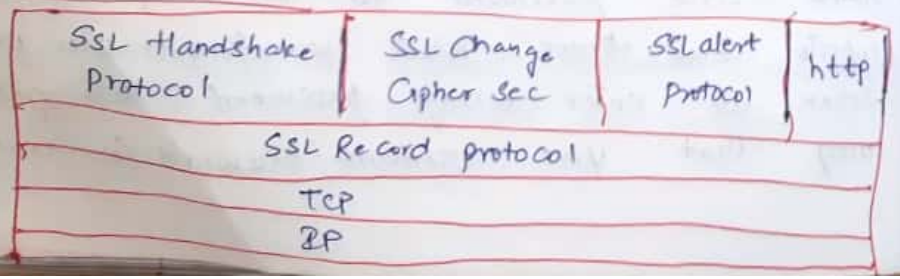
Secure Socket Layer (SSL):- It is used to provide Security for communication between 2 users. when 2 users are communicating each other inorder ensures the security that the msg in not altered, that the msg is not deleted, the msg is not known to third person. So inorder to ensure secure that travel safetly from User A to User B we use Secure Socket Layer protocol (SSL).

→ It ensures Integrity, authentication and confidentiality of the msg.

→ It lies between application layer and transport layer of TCP/IP.

→ In this Application Layer and Transport Layer in between we are having SSL.

Protocol Stack of SSL:-



→ SSL Record Protocol:- It has 2 services
1. Confidentiality → the message is not known to the third person. we can get by encrypt
2. Message Integrity → we get by MAC.

Working:-

Step 1:- In Application Layer data the data is present in this. this application Layer data is divided into no. of fragments. This process is called Fragmentation.

Step 2:- So, it is divided into no. of fragments. Based, on the size of the data it is divided into no. of fragments. the size of each fragment is equal to 2^{14} byte block

Step 3:- For each and every fragment we will do the process. we will take fragment and we will do data Compression for it. Data compression means reducing the size of the data. This compression has to be loss less compression. the data will not be lost but size will be reduced.

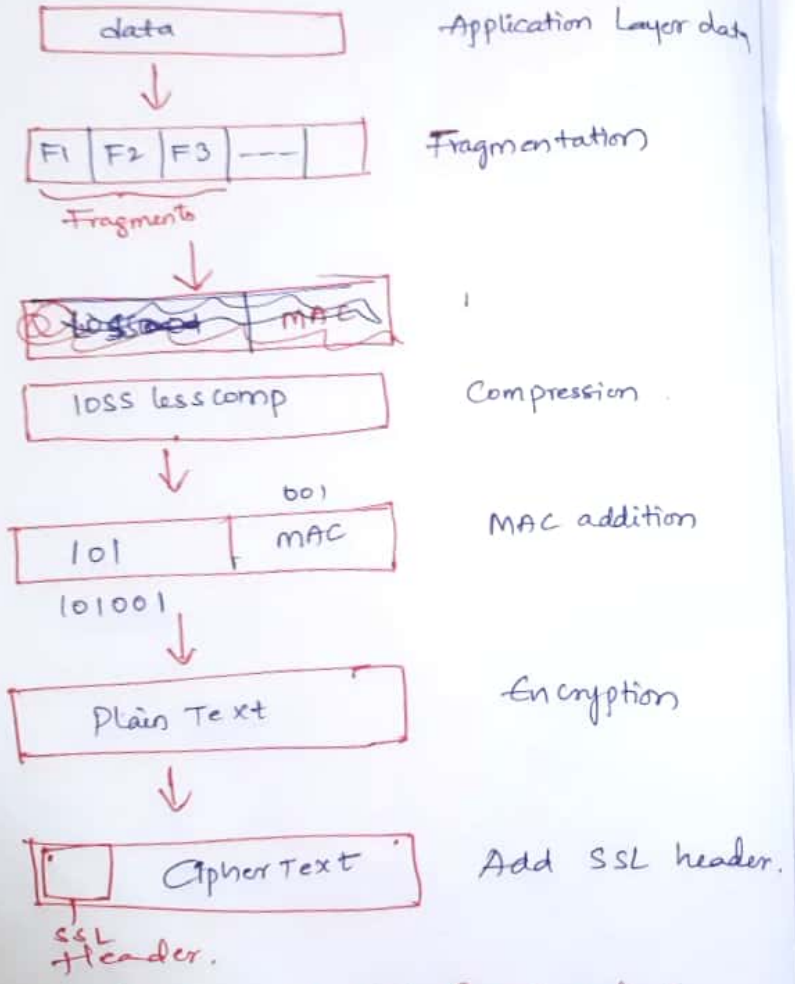
Step 4:- Calculate the MAC Code for the above data and MAC Code is added at the end. For above data we should add the MAC code. Why we are doing MAC addition means inorder to ensure the message Integrity.

Step 5:- Encryption is for Confidentiality.

Scanned with CamScanner

Before Encryption we call the data as Plain Text.

Step 6: Once we do Encryption we get Cipher Text CT. For this Encrypted data we should add SSL header; we should join beggining at CT.



Working of SSL Record protocol

SSL Handshake Protocol:-

⇒ It ensures Authentication.
→ most complicated part in SSL.
→ Key exchange b/w Client and Server.

Working:-

1. Connection establishment with Server.
2. Server will send Key to the client. 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 ⇒ Single byte (1 byte)
→ It copies the pending state into current state.

SSL ALERT PROTOCOL:-

→ Alert means notification.
→ Alerts related to SSL are sent to Clients.
→ It has 2 bytes.

byte 1 → Can have value as (1) or (2)
1 - warning 2 - fatal Error (terminate) means Stop the Connection.

byte 2 → Specifies the type of error.

Scanned with CamScanner

Transport Layer Security (TLS):

→ defined in RFC 2246

→ Transport Layer Security is needed for providing Security in Transport Layer

→ When data is travelling from Transport Layer to the next level or below level we need security to provide security the data should not be lost.

→ Inorder to provide Security we use Layer.

→ It is derived from SSL.

→ In SSL we use Hand Shake Protocol

→ TLS will depend on SSL Handshake protocol.

→ It provides a Secured Connection b/w client and Server. (i.e., No third parties).

→ TLS is used by http, Smtp.
↳ Inorder to ensure the Communication we use this protocols.

Working:-

→ Uses client Server handshake mechanism.

→ We will be establishing Connection between client and Server. (It can be wired or wireless)

→ Step 1: The exchange of Keys b/w Client and Server. (It is done by Diffie Hellman Key Exchange Algorithm)

→ Step 2: Now TLS Protocol will open an Encryption Channel.. this is done by RC4/IDEA/DES algorithm)

→ Step 3: It also ensures that the messages are not altered (by MD5/SHA Algorithm)
The data is sent from TLS is not altered.

* RFC (Request For Comments) 2246 is similar to SSL

* HTTPS (Hyper Text Transfer Protocol Secure):

⇒ It is combination of http and SSL.

→ It is an additional layer of security which is provided by TLS/SSL.

Ex: Website starting with (https://)

→ It is more Secured when compared to http.

→ Why it is more Secure because in http the data is in the form of plaintext only.

→ http the Client Sends data in PT the Server again Sent it in PT only

→ https → data is in the form of PT & CT.
Encryption and decryption takes place.

→ Https belongs to Transport layer protocol.

→ It heavier than http bcz (It has an additional Layer of Security)

→ It Runs on port Number 443 of Server.

→ The Server will have different ports.

→ It uses a Certificate Authority (CA)

Scanned with CamScanner

→ It works on assymmetric PKI and uses different keys

1. Private Key :- It is available only on the web server and managed by owner of the server.

2. Public Key :- It is available to everyone (client and server)

→ HTTPS is slower than HTTP. (No conversion is made in HTTP). But in HTTPS we will convert PT to CT. We will encrypt, decrypt. So, HTTPS takes time.

→ HTTPS is having better performance.

Main Usage :- Banking websites, Login Credentials.

* SSH Protocol :- (SECURE SHELL Protocol):

↳ Protocol for operating network services over an unsecured network.

↳ If data is lost means easy it is unsecured network.

→ alternative to Telnet, FTP etc. (unsecured protocol)

→ It uses client server architecture.

→ It follows assymmetric key cryptography.

For, Encryption ⇒ Public key
Decryption ⇒ Private key.

→ It provides confidentiality and Integrity of the data

Working :- 1. The client sends request to server.
2. The server will check authentication of client with public key.

→ Server will generate random string and it sent to client. It encrypts the random string and sent to client

→ The client will decrypt the data using PVT key.

→ The decrypted data sent back to the server end the decrypted data acts as Acknowledgement

→ Once decrypted data sent to server, the server will get to know that he/she is trusted client.

→ Finally, once authentication of client is proved and confirmed for server end then SSH Tunnel is created.

SSH Tunnel :- It is a channel for communication between client and server.

→ Whatever the data client and server want to give will happen through SSH Tunnel.

→ That is why it is secure.

→ Nobody will enter and steel data from SSH Tunnel.

Inorder to Establish the Tunnel this is processed.

Scanned with CamScanner

Wireless Network Security:-

⇒ Wireless means Bluetooth, Airports etc... These are wireless Security.

→ Protecting wireless n/w from unauthorised users

→ These are wireless Network

→ This is very complex in working. Because, there is no End-to-End connection.

Factors Contributing to risks in wireless Network:-

1. Channel
2. Mobility
3. Resources
4. Accessibility

Diff Threats (Wireless n/w Threats):-

1. Malicious Association:- Wireless device is configured as trusted. To the users it is trusted device. So, i can connect to it the data will be Stolen. Once user connected to it all data which is related it is stolen by third party.

2. Adhoc n/w:- It is also a wireless n/w. There is no common access point. Because, there is no Security between them. Because there is no common point in the n/w.

3. Non-Traditional n/w:- Bluetooth, barcode readers they do not have much security.

4. Identity Theft:- For each & every person is having particular Identity. Each & every fruits & clothes having the Barcodes. Here, the attacker will observed the n/w traffic & he will find out the MAC address of the computer. Which ever the computer is using the wireless n/w he will on that computer he will observe the n/w traffic and that is on Google all that will be observed by the attacker & that attacker will steel the MAC address. If MAC address is stolen the computer is in Risk.

5. Network Injections:- Network Injection means so much of data will be injected to the network without the user will not known this much of data is injected to the n/w without users notice the data will be injected. The traffic is not filtered that means it is common to happen.

Measures for wireless Security:-

1. Signal hiding Techniques (SSID) Should turn off. You should assign cryptic names to them. Some names are not understand. Reduce the signal Strength to the lowest level.

Scanned with CamScanner

2. Encryption and Authentication Protocols
3. Use antivirus s/w and firewalls
4. Change Routers pre-set password -
↳ we have to change password. We should not use pre-set password.
5. Allow Only specific Computers to access to your wireless n/w.

Mobile Device Security :-

→ Mobile Devices means (Smartphones, Tablets, memory sticks)

→ the Security of mobile device is important part in network.

Threats :-

1. Lack of physical security controls
↳ Moving from one place to other place.
↳ we need Security because we are not at particular point.
2. Use of Untrusted mobile devices.
↳ We Should use trusted mobile devices.
3. Use of Untrusted n/w.
↳ Personal hotspot (Untrusted n/w)
↳ When we want to use n/w we Should Connect to Public hotspot Only. Not to Public (wi-fi)
4. Use of application created by [illegible] parties
↳ If any Unknown Organisation has created a application Eventhough application is easy to use we Should not use that
5. Interaction with other Systems.
↳ We Should not allow auto synchronization
6. Use of Untrusted Content (Like untrusted QR codes)
7. Use of location Services (GPS)
↳ when it is required we should on location Services

Mobile device Security Strategy :-

↳ How to Overcome those threats. Inorder to overcome
↳ There are 3 Elements in mobile device Security

1. Device Security :- The device which we are using that Could be Mobile phone, Bluetooth, Headset or Laptop which we are using that Security and privacy of that device is very important
↳ How to Ensure the Security privacy which have to follow & Unfollow are:
1. Jailbroken devices should not be used
↳ It means removing software restrictions that are Intentionally put in place by the device manufacturer.

Scanned with CamScanner

↳ auto lock enabled (If we are not using the device, then it automatically lock will be Enabled)

↳ Password / PIN Protection. (If we use any device we must provide password pin to it)

↳ Autofill usernames / passwords (It should be avoided)

↳ S/w and OS upto date.

↳ Disable location Services. (Whenever we are not using Services we should off the location)

↳ Avoid installing third party application. (Only secured trusted applications only should be installed)

↳ Security trainings should be given.

2. Traffic Security :-

Inorder to Secure the n/w traffic. Only allowing trusted traffic into the n/w. That is based on authentication and Encryption.

↳ All traffic in the n/w should be Encrypted. (without Encrypting we should not send any msg)

↳ All traffic should travel in Secured Channel (SSL / IPV6).

(Inorder to transmit your msgs you should follow the Secured Channel)

↳ VPN Should be used

↳ Strong authentication Protocols. (which will monitor the n/w traffic and if any appropriate things are found it will stop).

3) Barrier Security :-

↳ stopping

↳ Establishing barriers to prevent unauthorised Sources into the n/w. These below are 2 barriers

↳ Firewalls

↳ Intrusion detection and prevention Systems.

Scanned with CamScanner

UNIT-V

Combining Security Associations:-

Case1:- In this with Individual SA's we can implement either AH/ESP. but not both.

→ When both are required, we need to combine multiple SA's.

In this we have 4 combinations (cases)

Case1:- We will provide Security for end systems.

→ BCz Host is directly connected to SA's.

→ Here we are using Security associations.

means One/more SA's.

→ Next, this SA's will provide directly to the host.

→ Then Host is connected to Local Intranet.

→ In this Local Intranet is connected to Router.

→ From the Internet router will distributing n/w to the host.

Case 2:- Here, we are having Tunnel SA

↳ Here the Security is provided to Security Gateways

↳ Local Intranet is Connected to the Security Gateway.

↳ we use Single tunnel SA.

But, here SA is connected to gateways

↓

Connected to host (via local Intranet)

→ mostly used in VPN.

Case 3:- It is combination of Case 1 and Case 2.

→ Tunnel SA will provide Security to the Security Gateway.

→ Normal SA's will provide Security to Host

↳ In this it provides Security to both Host & Security Gateway.

↳ In this on both sides we have Tunnels

Case 4:-

Here, we have Tunnel SA and Only One side SA's.

↳ In this tunnel SA provides Security to Host and to the Security Gateway.

↳ SA (Security associations) provide Security to Host.

↳ Here, we used in case of remote Sensors.

Scanned with CamScanner

↳ Between remote Host & Gateway the Security is provided by Tunnel mode.

↳ Between remote host & Local Host the Security is provided by one or two SA's.

Security Associations (SA): Security Association is a Contract Shared between all the Entities before the start of Communication.

Entity: Whoever is participating in Communication they are called Entity.

SECURE INTER BRANCH PAYMENT TRANSACTIONS :-

↳ Which we use in day to day life

↳ Simply we can say Online Transactions.

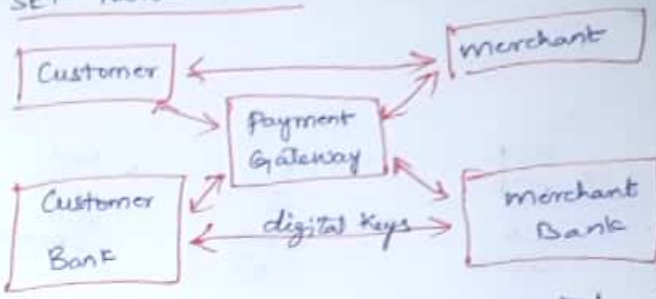
↳ It is done with the help of Secure electronic transaction (SET).

SET Protocol:- This protocol Ensures Security and integrity of electronic transactions (Credit card, debit, Net banking)

↳ SET restricts revealing of Credit Card details to merchants (Amazon, flipkart etc) So that data is protected from hackers.

↳ Implemented with help of digital signature.

SET PROTOCOL WORK



↳ Here digital Keys are generated. They will Confirm the certificates.

CROSS SITE SCRIPTING VULNERABILITY (XSS)

This is also case study.

↳ xss is a web Security Vulnerability.

↓

a type of injection in which malicious Scripts are injected into trusted websites.

↓

We are sending something into a Computer.

Ex: Data enters into a website/application through an untrusted source -(In term of a web Request).

↓

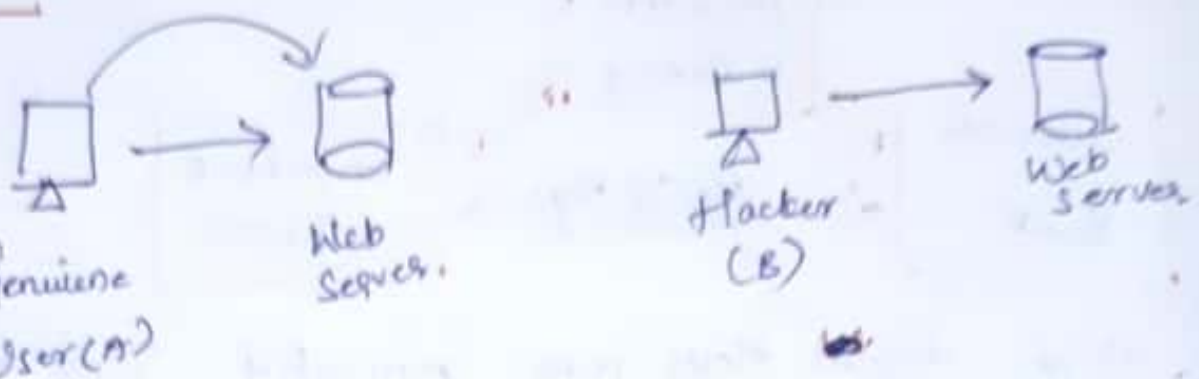
(Javascript, Html etc)

Hacker will give Username & password in the fields, he directly write Javascript & Closed. Then script will be executed and Some malicious will enter into our Web~~site~~ server

Scanned with CamScanner

⇒ The security of server will be comprimised this is Web Request.

Ex:-



↳ User will login with his credentials.
↳ Then hacker will login to webserver and he inject the code in it. The changes will be done.
↳ Next again User 'A' open and then hacker will made some extra thumbnails, Graphics is done on the web server. When User 'A' will open and attract to that thumbnails and he click on it. Then the confidentiality of User 'A' will be lost. It is known to hacker. He will know all the details of User 'A'. This will happens in Cross Set scripting. The security will be reduced.

Scanned with CamScanner