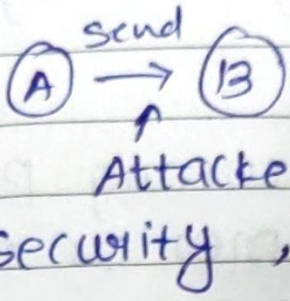
Web Security.

Chapter - 6.

Web security consideration.



To secure our data from attacker we need security, security is required for website

security considerth (~~sec~~ security way)

(1) updated software ⇒ Always update software.

(2) Beware of SQL Injecth.

SQL injecth ⇒ Attacker insert row, colm or inserting informath in form of table

⇒ so beware about all SQL injecth.
(any modificath by Attacker - SQL inject)

(3) Cross site scripting (XSS)

Attacker can will send Client script to your website like any detail related to client send to website and Hack website

e.g (1) user fill his/her detail through google form & informath stored in server, so server can reply your response is submitted

(2) Now, Attacker attack on dB to currupt the data, Fill wrong info., or ~~send~~ submite repeted google form with wrong detail to server.

(4) Error msg. - any error msg we need to carefully display when we are displaying.

e.g when i enterd wrong password so sometime pop up comes or msg comes you have enterd wrong username (OR) password.

or some server send msg you have entered wrong password.

In the 1st case attacker can't get whether username is wrong or pswd is wrong ⇒ then they can't attack.

Now in 2nd case attacker know yes their is only pswd wrong means username is correct, so attackes try to attack with apply the combinational pswd & attacks.

(5) Data validation ⇒ should be done from both side (client & server) data has to be validated for more security.

(6) pswd ⇒ pswd should be (strong) compilicated ~~not like~~ It should not like simple 123 etc. so attackes can't attack to the data

- cookies ⇒ when we entered in the website (Flipkart, Amazon, Javatpt) ↳ every website having a server where what we are doing in the website, which page we scroll all we store in File formate (cookies) so next time when we again visit to same website cookies will recommed the thing's what we searched before.

~~copy~~ cookies is dangerous.

Go the search engine setting and make "block cookies" so if trusted website want to ~~&~~ send something so it will not.

OR block third party cookies. (e.g Addvertisemnt etc)

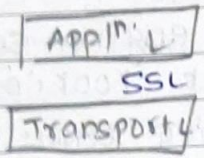
OR some website ask if you want to use cookies or not if yes than enter

* Secure socket layer (SSL)

(1) It provide security when 2 user are doing communicatn over on network so SSL give security bet 2 user.

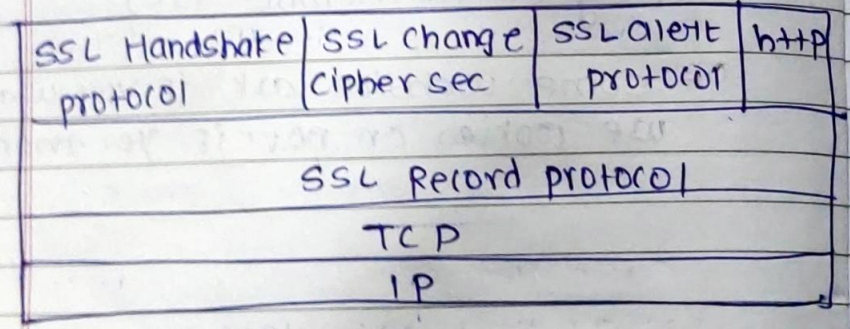
(2) It ensures the Integrity, authentication & confidentiality.

(3) It lies betn Applicatn layer & transport layer of TCP/IP proto.



TCP/IP → 4 lay
OSC → 7 layer

protocol Stack of SSL.

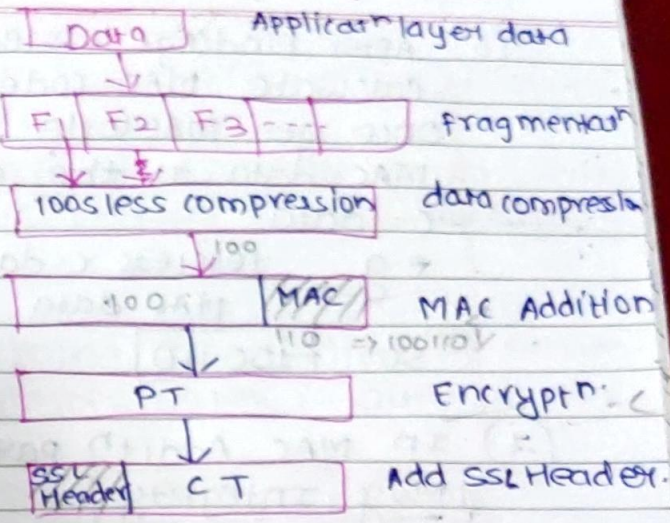


SSL Record protocol ⇒ 2 services.

(1) confidentiality of data ⇒ done by encrypt no 3rd party can involved.

(2) Msg Integrity ⇒ done by MAC.

working.



(1) A data present on Appln layer &

(2) data divided into no. of fragment and process called Fragmentatn. Based on size of data it's divide into Frg

(3) each fragment size = 2^{14} byte blocks

(4) Once it divided into no. of fragment each fragmet will follow same process.

(5) take F1 and do data compression (dc) dc ⇒ Reduce the size of data in F1

2 type dc ⇒ lossy c & lossless c.

lossy com ⇒ some data loss will happen ⇒ loss of data happen.

lossless dc ⇒ Data loss will not happen size of data will loss or compress

(6) After finding lossless data by comp. calculate MAC code
Once get MAC code Append (add) MAC data at the end of lossless c. data.
e.g lossless c. data = 100
MAC data = 110
so. 100110

(7) In MAC Addit^{n} part you will get Msg Integrity

(8) Before encrypt^{n} we call data as PT
Encrypt^{n} is used for confidentiality

(9) After Applying En on PT we get CT
(10) Once get CT → Add SSL Header at the begining (starting) of CT

(I) SSL Handshake protocol

we got Integrity & confidentiality in SSL Record protocol

Ensure ⇒ * Here we get Authentication.
* ⇒ most complicated part in SSL
* ⇒ It do key exchange bt^{n} client/serv

working.

(1) connect^{n} (wire or wireless) establish-ment with server.
(2) key exchange from server to client ⇒ for checking client is authorized or not
(3) key exchange from client to server ⇒ whether server is auth. or not
(authentication)
(4) Handshake done from server. ensure you are authorized person
e.g if you want to login in two gmail account.
1st step (1) GO to google enter gmail
(2) server ask for psod
(3) client enter psdod
(4) once write you access the login.

(II) SSL change cipher protocol
- size = 1byte → single byte
- It copies the pending state into current state.

(II') SSL Alert protocol
(1) whatever alert Related to SSL those alert sent to client.
(2) It has 2 bytes ⇒ size

2 byte.

1 byte ③ byte.

① If SSL give alert for byte 1 byte 1 have two value ① & ② If byte 1 give ① value than it mean warning

1 byte

If value-1 → gives warning

If value 2 → give fatal error

warning ⇒ something going wrong, phishing if not identify if still we not check warning than fatal error will occur means we have to terminate (comply stop connection)

② If SSL give byte 2 alert than it specify the type of error which is happing in byte-1

IV HTTP ⇒ self learning.
HTTPS ⇒ self learning.

★ SSH (secure shell protocol)

① Its used for operating the ntwork services over an unsecure n/w

② alternative to Telnet, FTP etc (unsecure protocol)

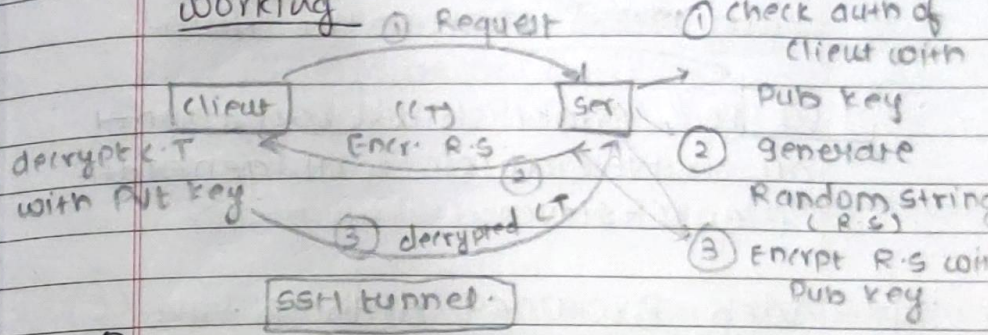
③ It's uses Client-Server Archite.

★ we can Access the services of unsecure network with full security (SSH)

④ It follows Asymmetric key cryptogra
for Encryption ⇒ use public key
for Decryption ⇒ use privdte key.

⑤ provide confidentiality & Integrity (CI

Working



① Client send Request to server
② once Receive request, server check authentication of client w.h. of pubkey
2.1 → once pub key will match i.e client is authorised person it will generate Random string (R.S)
2.2 → After generating R.S it will encrypt the Random string with pub key
2.3 → encrypted R.S i.e CT send to client
③ Now client decrpt the CT with client privdte key. (Refer above pt 4)
3.1 → client send decrypted data to server if all data correct hence server get's to know yes client is authorised person

of client

once Authentication is confirmed from server side than SSH tunnel (rest...

SSH ~~Chan~~ tunnel => It's channel for communicate betn client & server

So whatever data client want, server want all will go through SSH tunnel coz it's very secure nobody can enter into tunnel & steal the data.

So for establish of SSH tunnel all above process will generate i.e C-server

Web Browser Attack.

It occur when attacker exploit vulnerability. → take advantages of weakness

eg ① Atker target Organzn & enclues
② Atker inject malicious code → website
so Attacker attack on sensitive data
③ Attacker convert legitimate user into attacker's => very authorized person in orgnaizatn.

Attacker inject ~~code~~ Malicious code into their website & make them guilty person.

Web bug

① Web are tiny, small, invisible, graphic image or HTML element that are used to track the online activity of a user.

② They are usually attached with / in email or web page, & their purpose is to collect informatn about the user's browsing activity
e.g ① websites visited
② durath of each visit
& ③ other behaviour data (what searching

③ Now whatever info. collected by bug is sent back to entity that placed the bug for analysis & tracking purpose.

eg → Email web bug.
There is 1x1 pixel image attached with email, when Receiver open the email & download the email & send a request to server to hosting the image.
The Request include all info such as Receiver ip add, time of email open ser sotlw / Applⁿ for using the email

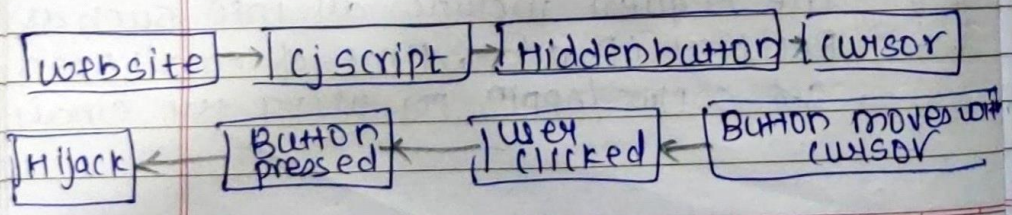
Clickjacking ⇒

It's one type of attack, where normal user is trapped to click & his clicks are bijacked by attacker without his permission.

Attacker use cj to steal sensitive info, spread malware, & execute unauthorized action on behalf of victim

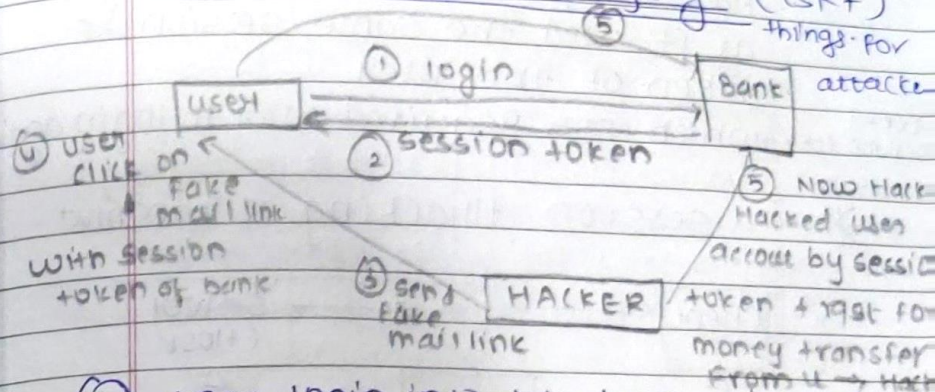
e.g Attacker create one website that contain button or link like "Click here for free gift".

→ when user click button or link, actually they are clicking a hidden button on a different website.
→ This's hidden button perform malicious action
e.g → posting msg on social media without his/her permission
→ making unauthorised purchase
→ downloding malware from user device



forgery ⇒ making crime (bad) strategy.
1 kind of attack - It force user to do the unwanted things for attacker

Crosssite Request forgery (CSRF)



(1) user login into his bank with username and password.
(2) Bank give user a session token like (yes you are entered or ~~login~~ page Bank dB page will see to user
(3) Sender will send user mail with malicious link that link looks like trusted location but actually it will connect to user bank
(4) so user click on fake link and uses the session token
(5) The hacker request is executing in user account i.e hacked user account by hacker
e.g money will transfer from user → hacker to hacker Account

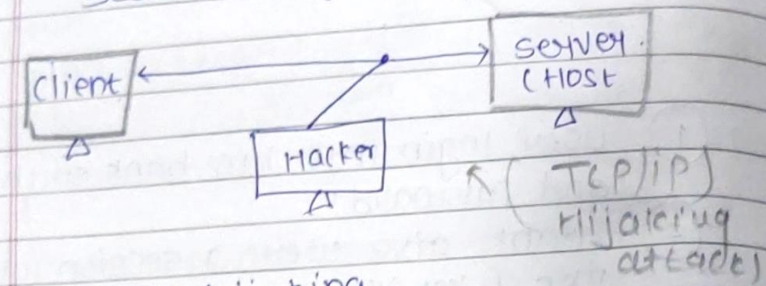
so How it happen (money transformation)

In attacker force user to perform action that they do not intend to perform (Changing pswd, sending msg, ① submitting/alt Record, submitting transactn, purchasing prod)

Hacker Request to Bank was forged as it used the same session token of the user which not Required user to login again

Hacked session token → which not Required user to login again

* session Hijacking & mngmnt



steps in hijaking

① Sniff the network
observe who is user, who is Host & network

② monitor packet flow betn 2 machine
① client login into with user id / Pswd with IP add to server, than server send session token to user

Attaker take both ip address of user and server while observing

③ kill the connection of user system
④ take over the session token through user IP add
⑤ now Attacker Act as user and start injecting spoofed packet to server

* Session Hijacking level: This level target on network, ip add, port

(I) network level - eg ↓ ⇒
e.g ① TCP IP session hijacking
② man in middle attack ⇒

Attaker intercepts and alters communictn betn 2 parties. The attacker can ~~drop~~ modify or block the commn without the parties being aware.

③ Man in browser attak

Here Attaker infect the target web browser with malware, or injecting a antivirus in browser, so this malware allow the attacker to modify, steal or redirect information from browser.

(II) Applicatn level eg.
① Brute force attack

This attack target the application login page [login]

→ In this attack guess the login pswd(Id) or session token again and again
→ For getting session token it attemp to many possibility until the correct one is found.
- In this Attacker repeatedly tries different session ID until they find one i.e valid, giving them access to user session

* Session Hijacking detection

(1) Manual Method ⇒ wireshark tools.
(2) Automatic tool ⇒ IDS (Intruction Detection System), and IPS (I preventary)

* Session-hijacking prevention
use antivirus for prevention.

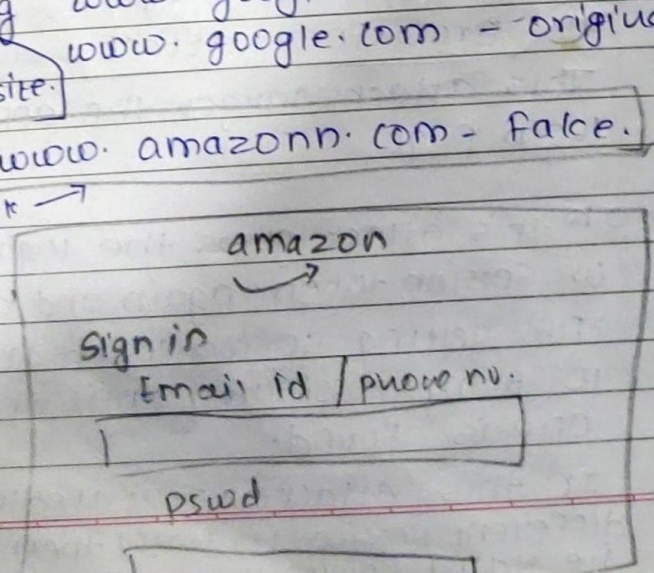
* phishing technique.

P. Attac -
(1) It's one kind of attack,
(2) It's aim to obtain the sensitive information like username, pswd, bank detail etc. by using fake website, email, msg etc. which look like original

(1) e.g www.googl.com - fake
eg phiss throug website. www.google.com - original

https://www.amazonn.com - fake.

when click →



(1) phishing through website.

support@sbionline.com
support@sbioniline.com - Fake.

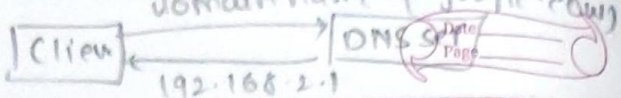
attaker
They send msg through email that update account. when cliks click to update on fake link all information attakes can will optain.

phishing techniques.
(1) session Hijacking.
(2) content injection - its kind of tec
where phisher change the part of content on the page of website.

(3) vishing (voice phishing)
(1) In phone phishing, phisher makes phone call to user & ask the user to dial no.,
(2) the purpose is to get personal info of bank account through the phone.
(3) phone phi. is mostly done with call fake

(3) Smishing (SMS phishing)
phi. conducted via SMS, a telephone based text msg service.

(4) link manipulation - phi send link → website
when user click on website link, it opens phishe website instead of website mentioned in link



* DNS attak. - Domain name server

It's convert alphabetical word (google) into IP add.

Top level 1st level ⇒ .com, .org
2nd ⇒ domain name (google)
3rd ⇒ host.

www.google.com

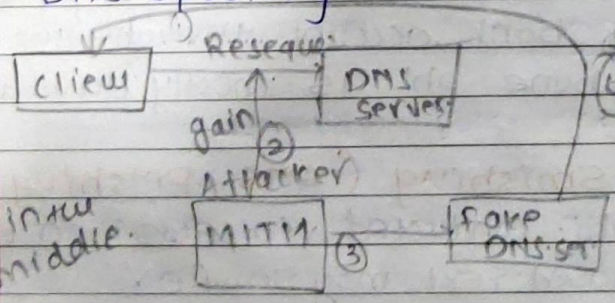
* DI in DNS attack

Server
google

1. Attack target the servers which contain domain name.
2. 2nd attack determine vulnerability of system & exploit them for their own good.

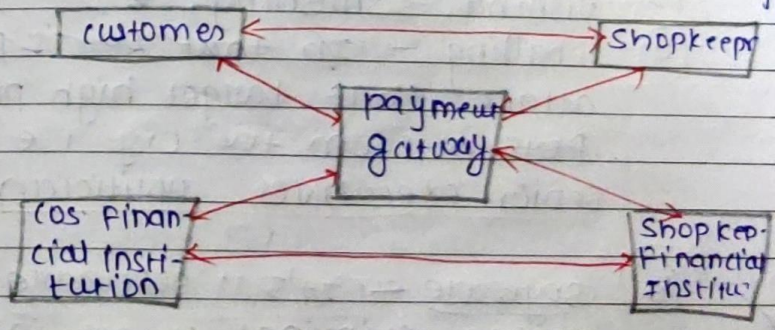
types:

1. DOS (Denial of service)
2. DDOS
3. DNS spoofing



* SET - (Secure electronic Transaction)

1. whatever the transaction we are doing in online mode (gpay, Paytm, phone) that transaction is secure by SET.
2. SET provide security, integrity & confidentiality to our transaction All transaction.
3. All transaction is done by SET
4. ~~&~~ SET uses different Encrypth & hashing techniques to secure all type of traction over the internet.
5. It also provide security like Visa, mastercard with help of S-trowsth technology (STT) & SSL ⇒ make more strong



1. Customer want's to transfer money to shopkeeper Account.
2. Both cust Bank account & shopkeeper bank account are connected to payment gateway.