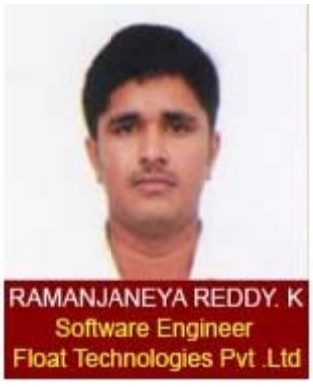
Attacks & Hijackings

CONTENTS

1. Buffer Overflow
2. Format string vulnerabilities
3. TCP session hijacking
4. ARP attacks
5. Route table modification
6. UDP hijacking
7. Man-in-middle attacks



Introduction:

The internet revolution made huge blocks of information available at one click and thus creating an information revolution. However, at the same time, the development has alarmed big concern for data security from various types of masqueraders. As a result, information security has gained more attention from individual level to organization level. Today, information security is the primary goal because information is valuable. We have to initiate necessary security measures to safeguard the information from diversified attacks.

In this chapter we are going through the different types of attacks and how the attacker targets the targeted system. Ways to prevent the different types of attacks and hijackings.

Buffer overflow:

Buffer overflow attack is one of the top most attacks used by the hackers. Hackers forcefully write the program to store the large amount of the data in the buffer, which is beyond the actual size of the data that stored in the buffer. At that time data may leads to the buffer overflow and corruption of the data.

In 2000, buffer overflow attack was found in Microsoft Outlook and Outlook Express. The Program had some loophole that will be the entry point for the attacker to conciliate with the system and simply sending emails.

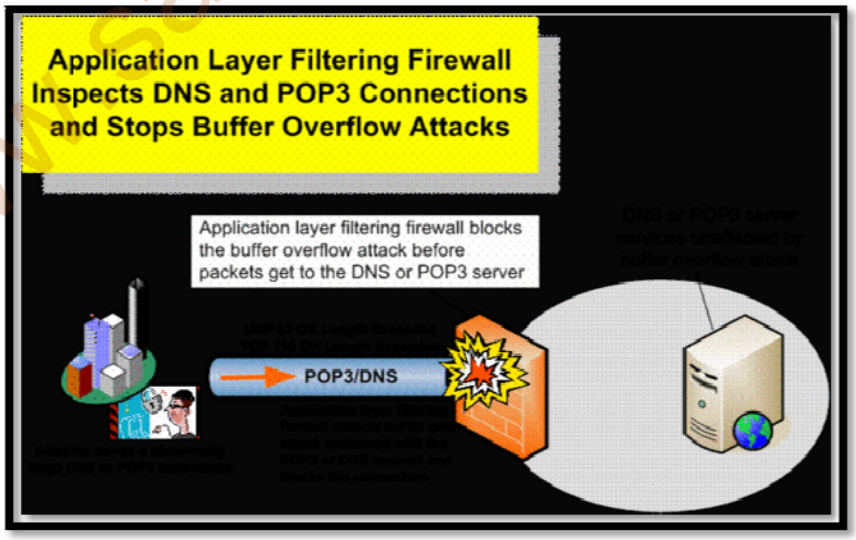


Figure: Buffer over flow Prevention

Prevention: "Prevention is better than cure."

- While writing the code, we have to prevent the usage of libraries. If there is any weakness found by the attacker in the library, this may lead to the buffer over flow attack. So we have to prevent the usage of libraries while writing the code.
- We can reduce the attack by filtering the code. We have to filter the user input code. In PHP we have to reduce special characters and have to replace them with readable characters.
- Before deploying the applications we have to test the application thoroughly. Sometimes if we deploy the applicationwithout testing it may leads to the application crashing.

2. Format String vulnerabilities

Format string vulnerabilities will occur when user submits the incorrect format string.

Format Function	Description
fprint	Writes the printf to a file
printf	Output a formatted string
sprintf	Prints into a string
snprintf	Prints into a string checking the length
vfprintf	Prints the a va_arg structure to a file

vprintf	Prints the va_arg structure to stdout
vsprintf	Prints the va_arg to a string
vsnprintf	Prints the va_arg to a string checking the length

Below are some format parameters which can be used and their consequences:

"%x" Read data from the stack

"%s" Read character strings from the process' memory

"%n" Write an integer to locations in the process' memory

Common parameters used in format string attack

Parameters	Output	Passed as
%%	% character (literal)	Reference
%p	External representation of a pointer to void	Reference
%d	Decimal	Value
%c	Character	

%u	Unsigned decimal	Value
%x	Hexadecimal	Value
%s	String	Reference
%n	Writes the number of characters into a pointer	Reference

If an attacker will pass a format string consisting of printf conversion characters (e.g. "%f", "%p", "%n", etc.) as a parameter value to the application, they will execute as

- Execute arbitrary code on the server.
- Read values off the stack.
- Software crashes.

Format string vulnerabilities using printf

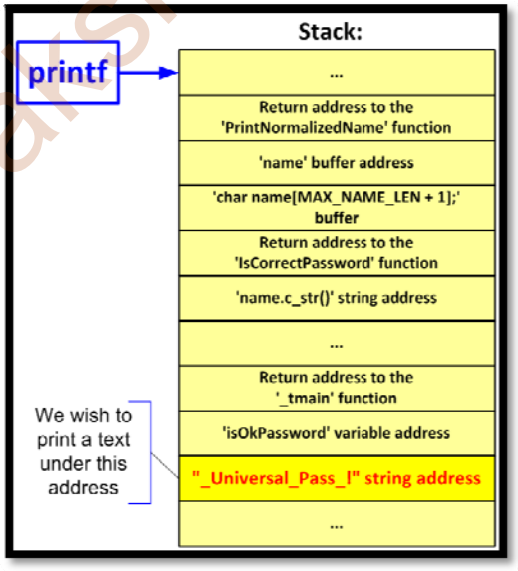


Figure: Format String Vulnerabilities using printf

3. TCP Session hijacking

TCP session hijacking occurs when the attacker takes the TC session between the two computers after gaining the access, and then becomes the authenticated to the system. Most of the hackers will attack stealing the IP packets.

Attacker will intrude in to the conversations and encourage it by sending the IP packets. If source-routing is turned off, the hacker can use blind hijacking, whereby it guesses the responses of the two machines. Thus, the hacker can send a command, but can never see the response. However the attacker will send the sniffing packets between two machines to get the response from the machines.

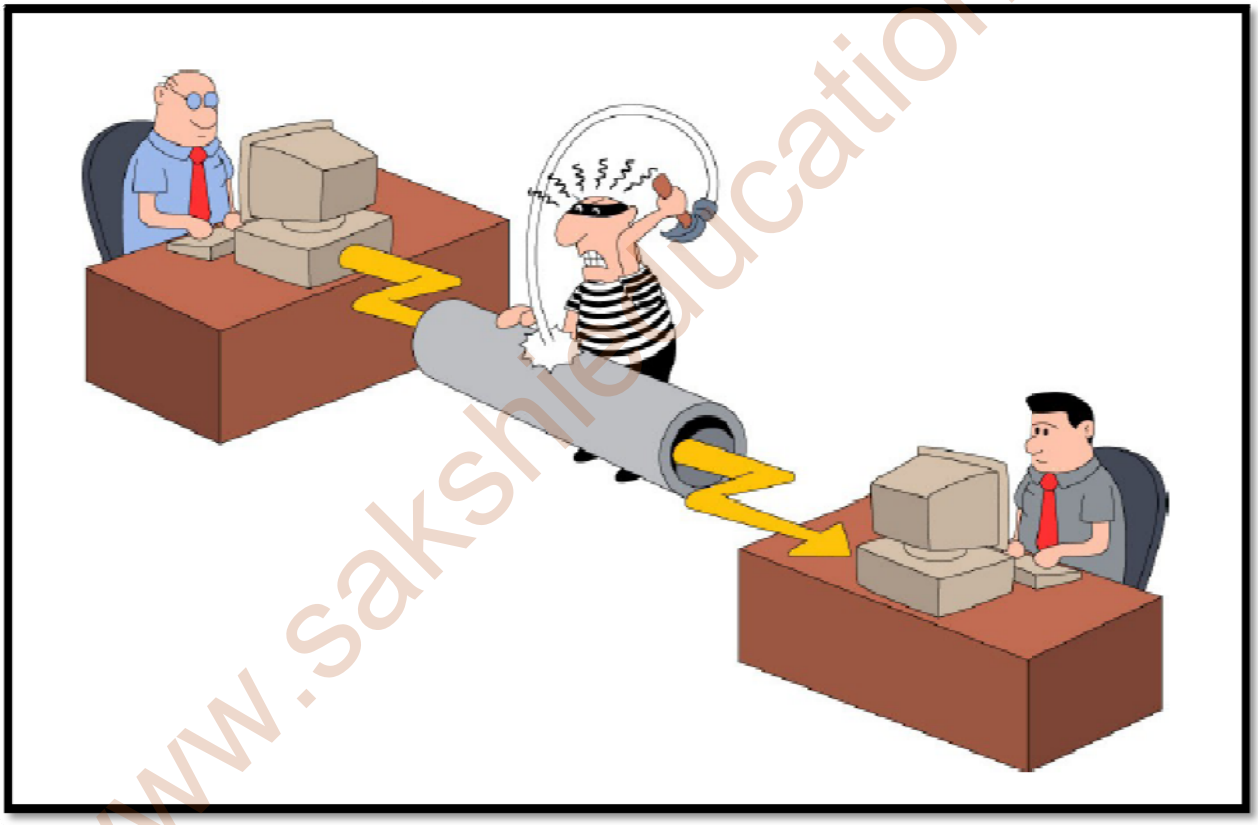


Figure: TCP session hijacking

When the destination routing is disabled, which is the case these days for most of the equipment, a second method involves sending packets as "*blind attacks*", without receiving a response and trying to predict sequence numbers and malicious IP packet. The stolen IP packets are used to read the confidential data.

4. ARP Attacks

ARP Spoofing is a type of attack in which a hacker sends fake information ARP (Address Resolution Protocol) messages in LAN. This fake information will get access to the target system and this in turn will be linked to the attacker's IP address in the network. Once the attacker's MAC address is connected to the targeted IP address, the hacker will start receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify, or even stop data in-transit. ARP spoofing attacks can only occur on LAN that utilise the ARP.

ARP Spoofing Attacks

The impact of ARP spoofing attacks can have serious implications for the organisations and companies. In their most basic application ARP spoofing attacks are used to steal the sensitive information.

- Denial-of-service attacks
- Session hijacking
- Man-in-the-middle attack

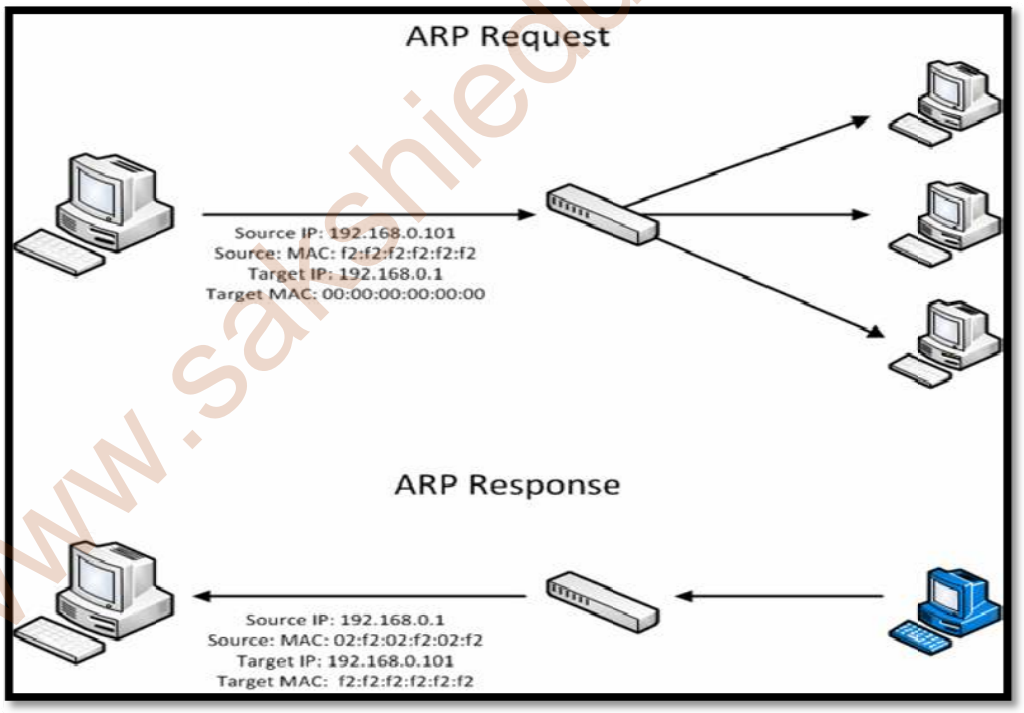


Figure: ARP Spoofing

5. Route table Modification

There are two types of attacks in route table modifications:

1. Misrouting Attack
2. Blackmail Attack

Misrouting Attack

In Misrouting attack, unauthorised router sends the data packets to the wrong destination. At that time, triangle will be formed between the routers. Packets will be sent to the wrong destinations. Attacker adds the number of virtual nodes to the route during the phase.

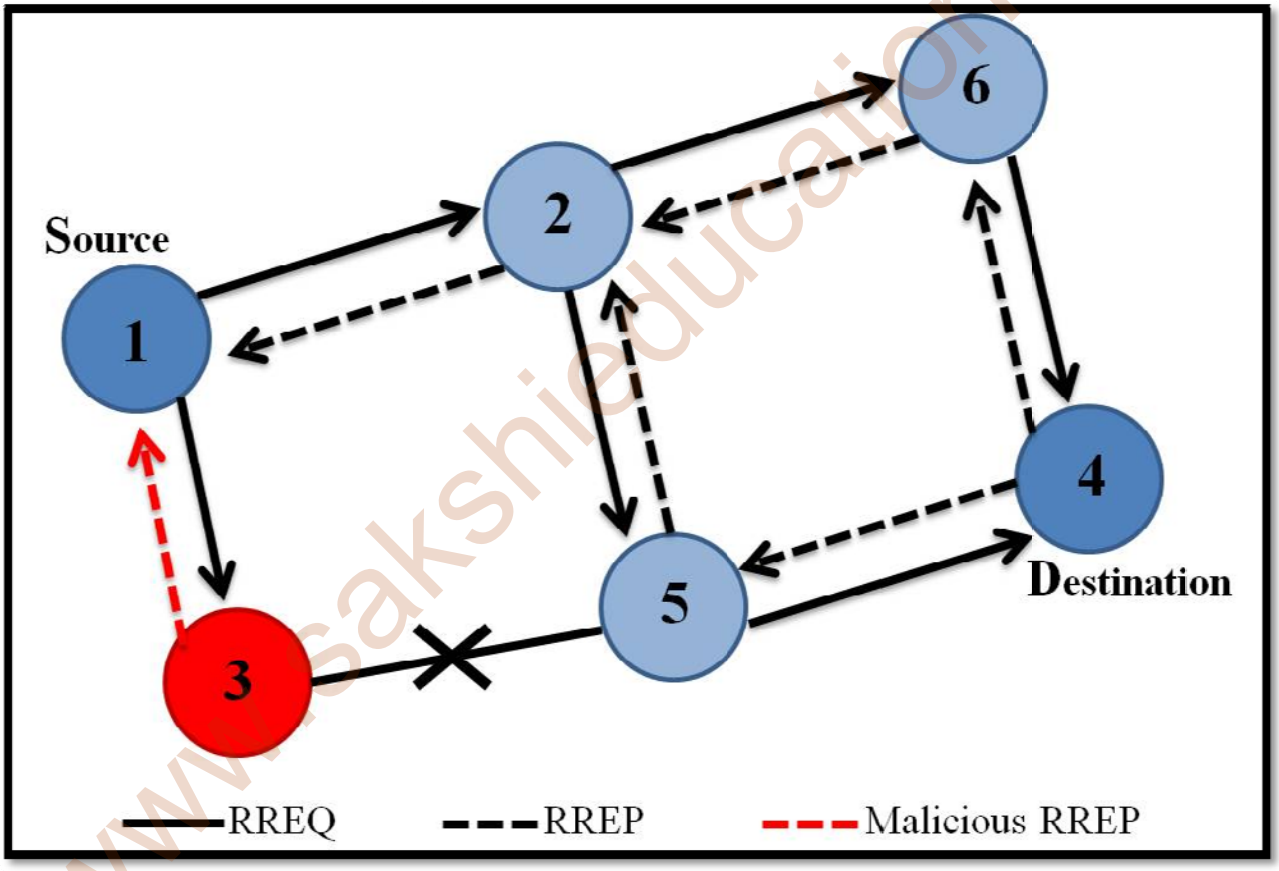


Figure: Misrouting Attack Example

Blackmail Attack: Blackmail attack causes false identification of a good node as malicious node.

6. UDP hijacking

- UDP stands for User Datagram Protocol.
- This is similar to TCP, whereas UDP attackers do not have to worry about the overhead of managing sequence number and other TCP mechanisms.
- Attacker will inject data into session without been detected is extremely easy in UDP.
- UDP is connectionless protocol.

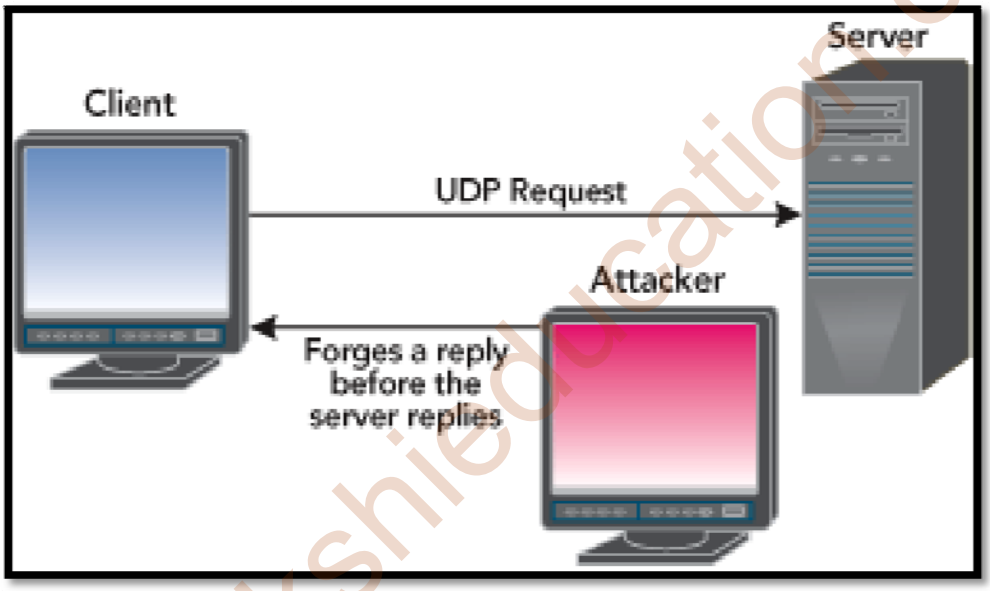
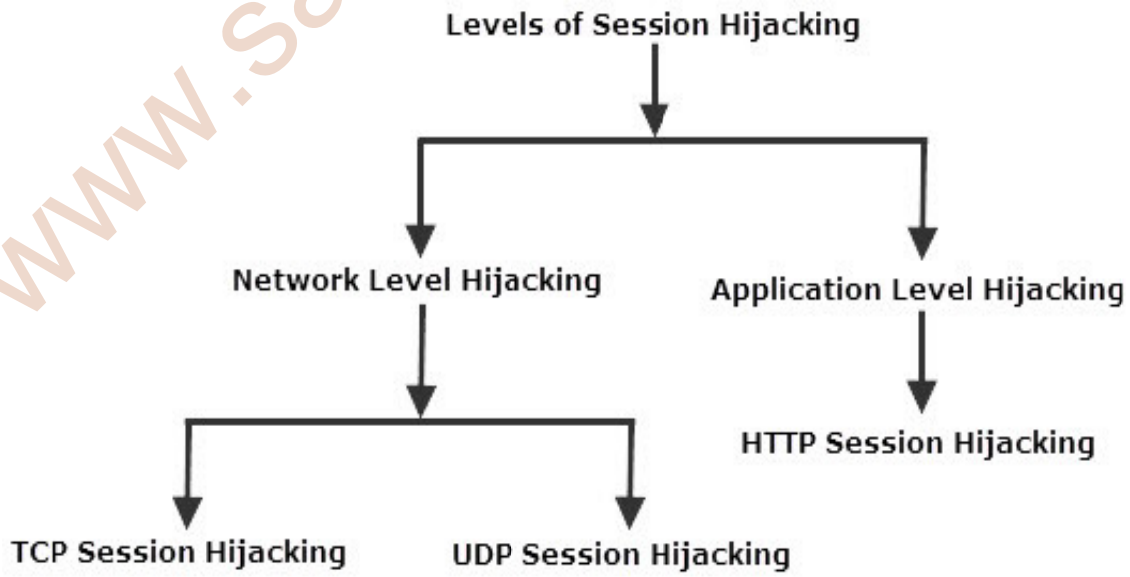


Figure: UDP Hijacking



7. Man-In-The-Middle Attack

- In the man-in-middle attack, the attacker will enter into the conversation by sending the malicious packets.
- After gaining the access to the conversation, the hacker will read the packets and send the malicious packets to the victim in the conversation.
- A man in the middle attack exploits the real time processing of transactions, conversations, or transfer of other data.

Man in the middle attack tools:

- Packet Creator
- Ettercap
- Dsniff
- Cain e Abel

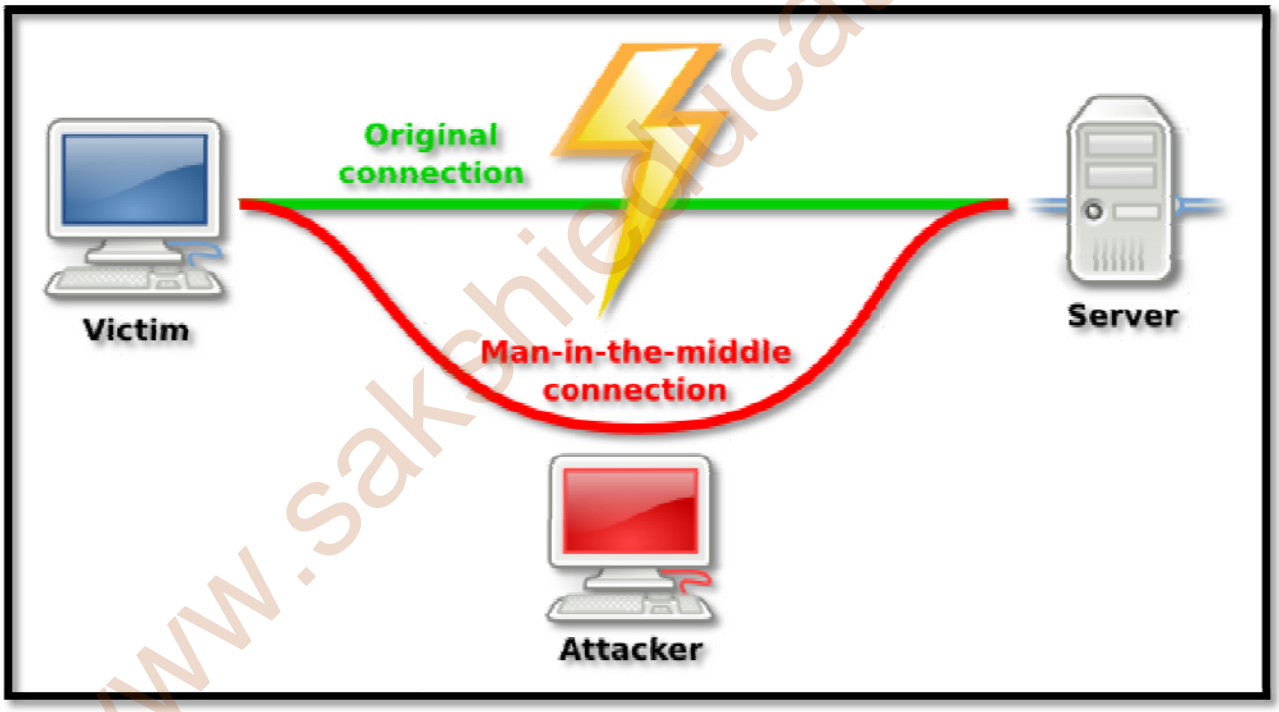


Figure: Man in the Middle

Security Measures:

- We have to use strong encryption between the client and the server.
- In this scenario, sever authenticates the client by sending some digital signatures, only after that connection would be established.
- Never connect to open Wi-Fi connection.