International Journal of Engineering & Technology, 7 (2.6) (2018) 193-198

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Session Hijacking and Prevention Technique

Anuj Kumar Baitha*, Prof. Smitha Vinod

Christ University,
**Corresponding author E-mail: anuj.baitha@mca.christuniversity.in*

Abstract

Session Hijacking is an attack which is basically used to gain the unauthorized access between an authorized session connections. This is usually done to attack the social network website and banking websites in order to gain the access over the valid session as well as over the website too. These attacks are one of the commonly experienced cyber threats in today's network. Most of the websites and networks are vulnerable from this kind of attack. For providing the protection I have given the multiple ways to protecting from this session hijacking attack. I have especially focused on one of the major attacks in this session hijacking attack SSL Strip attack which play very vital role in this kind of attack. Sometimes this session hijacking attack is also known as the Man in the Middle attack (MIMA).In this paper, I have covered many security mechanisms to stay away and protect you and the network. This session hijacking attack is very dangers for the security perspective. Even it can steal all users' most sensitive data. This can create a big loss for the users financially. From all these types of attack, I have proposed many mechanisms to help the users to stay away from the attack. The main objective of this paper is to give detail information of session hijacking and countermeasure from session hijacking attacks.

Keywords: *SSLStrip, Session Hijacking, MIMA, vulnerability.*

1. Introduction

Cyber Security, one of the most major topics in this online world. There are various security threats that lurk the network every time in order to use the network vulnerabilities to harm the users. As this modern world, everything is connected to the internet network. Online E-Commerce is one of the most used by the customer for the shopping and the online transaction. Banks provides easy ways to manage the online account and online payment which makes the people life easy and fast. People blindly rely on online transaction and payment. While doing online transaction sensitive information passes through the internet and the confidentiality and integrity really have become a big change for to maintenance, this is very hard given to protection each and every sensitive information. We need to develop the most secure mechanism to handle all this problem which can give us assurance to keep away all threat from users confidential and sensitive information of users. Some of the security threats like Man-in-the-middle attack, Denial-of-service (DOM), sniffing, ARP spoofing, SQL injections, Phishing attack and much more which has malicious intention to get used of the vulnerability of the network and the web application for the bad intentions. Apart from this Session hijacking is one of the commonly used to attack by numerous attackers around the world on the internet network. Session Hijacking plays a major role to steal the confidential and sensitive information which passes through the network. It has the capability to steal the information without the knowledge by the users. There are many ways to perform this session hijacking attack and one of the most used attacks is Man-in-the-middle-attack. In this attacker put himself between two trusts worthy connection and steal all the important information which is being done by two systems. Using session hijacking attacker attacks so smartly so that victim can't even think that someone is stealing his/her information. Session Hijacking has a capability to perform the attack without giving any warning and any changes in the data or information. Because of that victim can't even imagine that some have attacked in his/her system an attacker can easily get all the information which attacker wanted, this is the big advantage for the attacker that session hijacking give all the features to fulfill attackers intention without getting caught while doing attack, which gives them more motivation to do more attacks.

As we are looking into session hijacking attack it is necessary to know background details about session hijacking and how it works.

As we have seen in the introduction of session hijacking it is the process of taking over the unauthorized already created trusted and valid session between two system connection in order to steal and compromise user's confidential data and this also known as a man-in-the-middle attack. When someone who logins into any web application it creates a trusted session between a client and the web server by using the three-way handshaking. Three-way handshaking is a process which provides the way to create a trusted valid connection using the session between client system to a web server and after making a trusted and secure connection then only client and server start communicating with each other and send the receive data. In session hijacking attack attacker take over the valid trusted connection send packets to a server as a genuine client and send receive the packet from the server and send to the client as a genuine server. The big advantage of session hijacking attack is it does not have to break any defense or security firewalls just it need to keep listening to the network and take over any valid session. There are basically three type of session hijacking attack which does the same work in different ways. We see all three types of session hijacking in brief which will give us more deep knowledge about the session hijacking attack and its methods.

Three types of session hijacking are:

- Active session hijacking
- Passive session hijacking
- Hybrid session hijacking

1.1. Active Session Hijacking

Active session hijacking is a technic in which an attacker attacks in already active session between user and server. Attacker attack in an active session and put off the valid user and put himself in place of a valid user using Denial of service attack (DOS). Before doing the DOS attack attacker sniffs the connection and captures all the data packets between user and server using some packet capturing tool like Wireshark. Denial of service attack in which attacker flooding the target with traffic, attacker send lots of request or information to the target network and make unavailable for the server because of that target system can't be able to use the services which is sent by the server side and after sometimes target machine get shut down or get crash in order to unhandled the traffic flood. The server waits for sometimes and send a request again to user machine for the connectivity and at that moment attacker masquerade and accept as a valid user and send the acknowledgment to the server and attacker make a connection with a server in place of a valid user. The active session hijacking diagram is given fig.1 that illustrate better active of session hijacking [1].

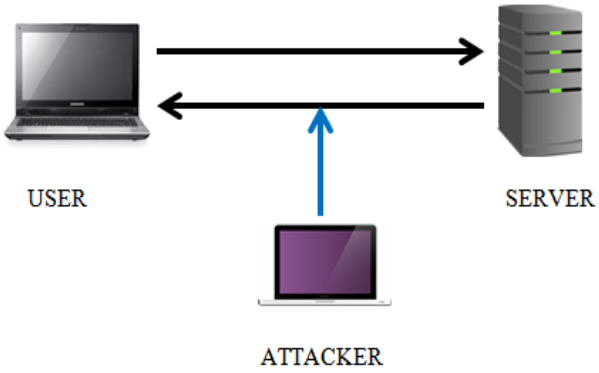

Fig. 1: Active Session Hijacking

1.2. Passive Session Hijacking

In Passive Session Hijacking attacker put himself between valid user and server and attacker send the valid packets to the user masquerading as a server and receive the packets from the user and send to the server masquerading as a valid user. In this Passive Session Hijacking attack attacker can all the data pass through the attacker system an even attacker can make some changes on the data packets and neither user nor server can detect the changes in the data packets. This way attacker can gain all the required details for his/her mischievous works. But there is one disadvantage for the attacker. He/She can only access the data between user and server until and unless a session is active if any chance user signs out or server reset the connection by any reason attacker will not be able the access the data packets and session will be terminated permanently [1].

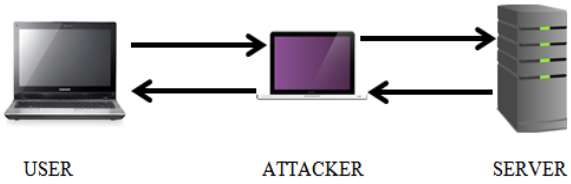

Fig. 2: Passive Session Hijacking

1.3. Hybrid Session hijacking

Hybrid Session Hijacking is the combination of the Active Session Hijacking and Passive Session Hijacking. In this attackers user both types of session hijacking technique to achieve his/her goal it can be Active and Passive. Hybrid Session Hijacking can be divided into two types which are given below:

- Blind Spoofing Attack
- Non-Blind Spoofing Attack

1.3.1. Blind Spoofing Attack

Blind Spoofing Attack in which attacker attacks the target system without any changes in the connection between the server and the victim machine. An attacker simply captures the entire packet from the network between user and server to find out the TCP sequence number in order to get the authentication with the server and get the full control over the session. But in this attack there is big problem it is very difficult to find out or guess the TCP sequence number through captured packets because TCP sequence number is random number each time it generates the new and random TCP sequence number which make it very hard to find out the correct sequence number it needs lots of time to find out and for that attacker need to keep on capturing the packets to analyze the TCP sequence. For finding out the right sequence number it may take a long time or attacker has to wait with patience to get success in these types of attack [3].

1.3.2. Non-Blind spoofing attack

Non-Blind spoofing attack in which attacker should be on the same network as well as he/she should be under the same subnet also where an attacker can monitor the traffic between victim and server. This is easy for the attacker to monitor the traffic from the same network because the attacker can see the packets traveling through the same network. Attackers keep on monitoring the connection and try to guess the TCP sequence number of the next packets in order to get authentication over the connection using the TCP sequence number. Attackers find the correct sequence number and re-establishing the connection based on correct sequence number with the server. But the big problem on this attack is today's routers don't allow to broadcast the packets in the network they keep it turned off in order to protect the packets. For shorting out this problem attacker make the connection reset in order to put him between routers to capture the first broadcast packet [3].

In application level the attacker attack and hijack the session as well as try to create the new session with the newly created session ID. These sessions ID's can be gained by guessing or by the stealing from the connection using some packet capturing or monitoring tools. Using session ID attacker validates with the target machine to take over existing valid session or creates a new session using new session ID. [3].

The session ID is a unique number which is assigned by the server to the specific user during user visit to that website. The session ID is assigned inside the cookies form field or sometime in the field of URL [6]. There are many ways to generate the session ID some of the web servers generate the session IDs by incrementing static numbers, but the way of generating session IDs is not much suitable way and this is not much secure also, attacker can easily predict the session ID if the attacker is continuously monitoring the packets which are passed through the victim machine to server. Because this incrementing the static numbers is easily guessable by the attacker that's why the way of generating session ID is not suggested. The best way to generate the session ID is using the algorithm which makes the session IDs more complex and more secure compared to incrementing static numbers method, using

algorithms to generate the session ID that involves various complex methods which make session ID more secure and very hard to guess and predict by the any attacker, using algorithm it make generate more complex session ID and send it in an encrypted form so no one can understand and identify the session ID.

1.4. Stealing session ID's

There are many ways of stealing the session ID's some of them are given below.

1.4.1. Sniffing

Sniffing is one of the ways of attack in which attacker hijack the network steal the session ID. Attacker continues to monitor the victim's network traffic and tries to find out any packet traveling unencrypted form if the attacker finds out any packet without encryption then it tries to find out whether it consist session ID or not. If the attacker gets session ID the session ID inside the packet using that session ID it takes over already created the session between victim and server and an attacker has the capability to make a new session and get all the information of the target machine [3].

1.4.2. Brute Force

Brute Force is one of the famous attacks it has a capability to crack any character, number, symbols and special character combined username or password or any word. This Brute Force attacker may take so much time but give the assurance of completing the work. In this Brute force attack attacker can set the combination of the character, special character, symbols and number according to their requirement even attacker can set the number of words. Suppose victim has 8 digits of the password by guessing attacker set the length of password till 8 so this brute force check all the combinational word which is set by the attacker and till 8th digit. In this kinds of attack, an attacker need have lots of patience and time to make it complete. For cracking the session it this brute force attack in the target network and check all the combination set by the user to crack the session ID and give the correct session ID to the attacker and using that attacker take over the valid already created session [3].

1.4.3. Cross Site Scripting

Cross Site Scripting (XSS) is another way of attack to steal the session ID. This XSS is also known as the client side code injection attack, this code has a capability to execute the malicious script (malicious payload) into any website or the web application. This attack basically uses the vulnerabilities of the websites and whatever user input into the website it makes the input as unencrypted or uuencoded and sends that information to an attacker in the plain text. But there is a big disadvantage for the attacker is this attack only work for the vulnerable target these days many websites have been patched with these security issues [4].

1.5. Tools for session hijacking

There are many tools available for Session Hijacking

- Wireshark
- T-SightS
- Hunt
- Hamster and ferret

2. Attack Methodology

We are going to show session hijacking simulation in the virtual environment. We will set and install requirement operating system in VMware on host operating system. Requirement operating systems as follows:

- Victim Machine (Windows 7) Virtual Machine
- Attacker machine (Kali Linux) Virtual Machine

The Kali Linux is used as an attacker system and windows 7 is used as the victim's machine, in this attacker put himself between the victim machine and router to sniff the packets traveling through the network.

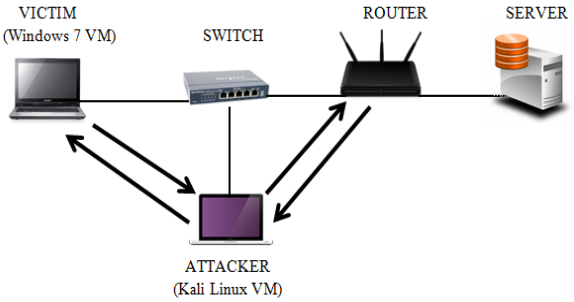

Fig. 3: Demonstrate virtual environment

We are going to demonstrate the session hijacking attack in the virtual environment and all the setups have been done both attacker machine (Kali Linux) and victim machine (Windows 7). The machine will provide the internet connection and private IP address will be assigned to both machine.

2.1. IP address

- Attacker's machine (Kali Linux) IP: 192.168.209.131
- Victim's machine (Windows 7) IP: 192.168.209.135
- Gateway Address: 192.168.209.2

2.2. Attacker machine setup

Most important thing is to setup the Kali Linux; we are going to setup Kali Linux for Men in the middle attack (MIMA) in between windows 7 and router where we will attack and put Kali Linux between windows 7 and router in order to sniff the packets.
First will check the connectivity between Kali Linux and Windows 7 using the **ping** command as shown in the figure 4:

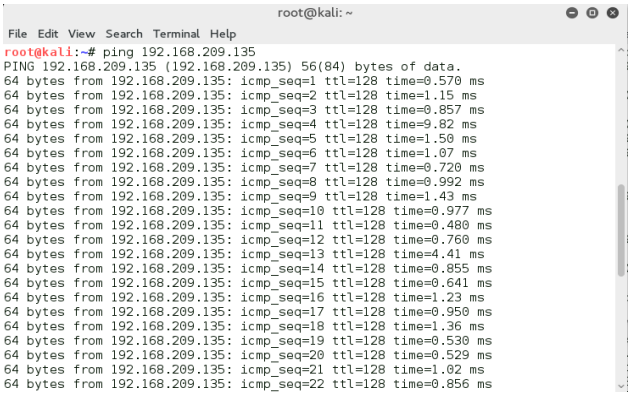

Fig. 4: pinging

If we get the ping from the Kali Linux to Windows 7 that's means connectivity is good between them without any interruption and attack can be done from here.
We are going to show main session hijacking attack with MIMA here we are going to attack and steal the HTTPS connection between Windows 7 and router using the SSL strip in the Kali Linux (Attacker machine). SSL Strip is a Script using that force victim to send the packets in the unencrypted form this SSL Strip remove the secure layer form the HTTPS and force to send in HTTP connection.

We have used sslstrip-0.9.2.tar.gz which is easily available on the internet. First of all, we need to do basic work like after download we have to extract (unzip) the SSL strip-zip file and we have to put that extracted file into separate place.
We will open terminal and set the location using cd command inside the SSL strip folder it will look like this as given below:

```
root@kali:~/sslstrip-0.9.2/src/sslstrip#
```

Now we have to forward the IP traffic which is generated in HTTP by using NAT forwarding in Kali Linux for we need to use a command which is given below:

echo 1 > /proc/sys/net/ipv4/ip_forward

We have to make some changes inside the sysctl.conf file it can be found the location of etc/sysctl.conf, we can go directly or we can us vi (Virtual editor) for editing the file just we find and uncomment the net.ipv4.ip_forward=1 line and save it.
Now we will setup the IP tables rules using a terminal in the Kali Linux, here we redirecting the traffics at the particular port number 8080 for that we will use this command given below.

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080

Now we have to setup the SSL strip for sniffing the network between Windows 7 and router, this will all the HTTP connection in the network. For setup we have to use the command as follows:

python sslstrip.py -k -l 8080

For working this command there must be python install into the Kali Linux. This is the most important command which listens to all the traffic which redirects through the port number 8080. For that we have to keep this terminal for the process for further processes we will use new terminals, this will remain open as shown in the figure.

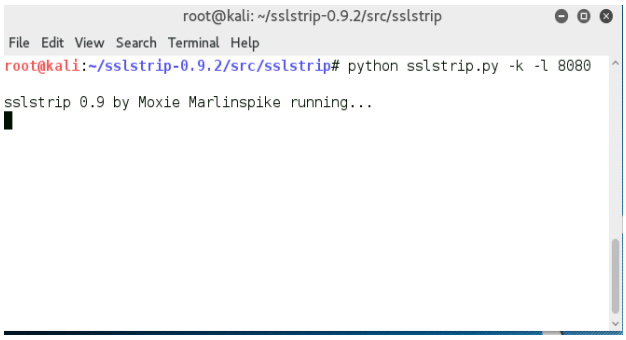

Fig. 5: Sniffing Network

Now we will do ARP poising attack and make the windows 7's traffic to pass through our created proxy server. APR posing is also known as ARP Spoofing this special done in the local area network to send the malicious ARP packet or we can say the unwanted lots of packet to the default gateway of the network in order to make changes in the pairing of IP to MAC(Media Access Control) address table of the network. This ARP Protocol has the capability to translate IP address into MCA address in order to make the attack on the network. We are going to attack in the target IP and the default gateway of the network using ARP poising attack for that we have command as follows:

arpspoof -i eth0 -t 192.168.209.135 192.168.209.2

In this above command, we have used eth0 because it is Ethernet and the first IP is target machine IP address (Windows 7) and the second one is default gateway IP address. After giving the command into the terminal we will leave terminal for the process this terminal keep on sending the ARP packets to the target machine and default gateway. As we can see in the figure.6 below:

Fig. 6: ARP Spoofing Attack

Now we will start the main attack into the windows 7 machine. We will see the victim machine activities before the attacking and after the attack figure shows the website before the attack into the machine:

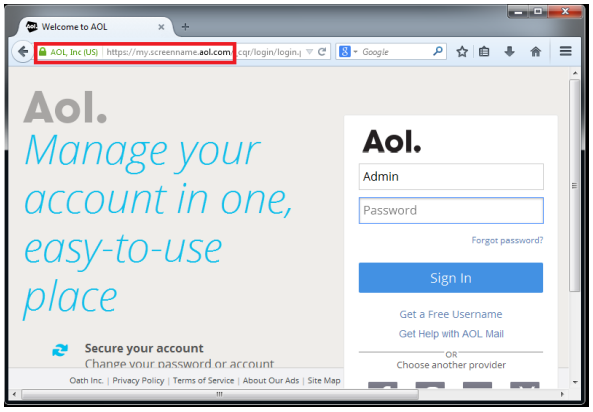

Fig. 7: Before Attack

We can see in the above figure URL it is in HTTPS with a secure connection, which shows that this website is secure and protected and whatever data input in the site will travel in the network in a protected manner and no one can see the sensitive information of this website.
Now we will give the attack command from the attacker machine (Kali Linux), we will open a new terminal and put new command:

urlsnarf -i th0

This urlsnarf command will sniff the all the URL used by the Victim machine and to the attacker with all the details like visiting website, link and many more details of the victim as shown in the figure.8:

Fig. 8: URL Sniffing

We will use next command to sniff the victim input data. So whatever victim will put on the website it will show to the attacker in the plain text command is given below:

ettercap -T -q -i eth0

We will give this command in new terminal and keep it open this terminal will display the user input details in plain text. We will see the after attack into the victim machine how its website looks like which is given in figure.9:

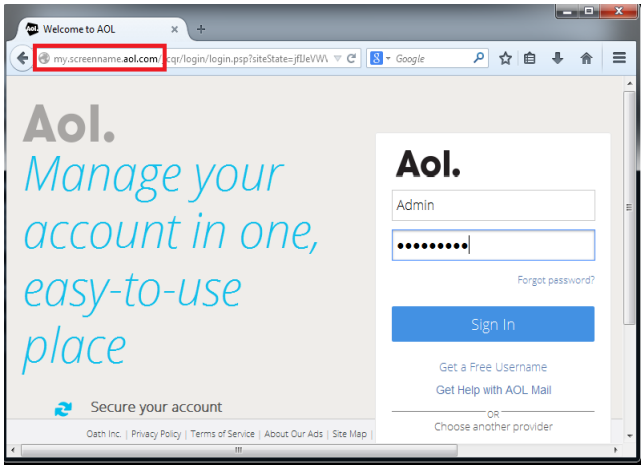

Fig. 9: After Attack login page

We see in the URL there is not more protected sign in available and there is no HTTPS secure site layer. It shows that our attack is working successfully and in the login panel we have entered username= Admin and password = 123456789. As we can see in the website login panel username is Admin and password we cannot see. Once the victim press the sign in button website will send the username and password to the server for the login. Now we will see the how this looks to attacker.

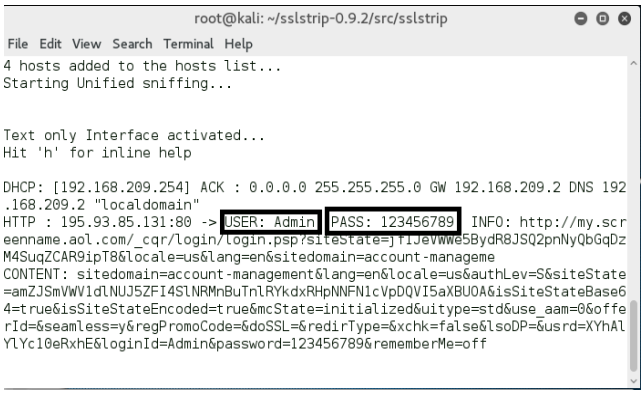

Fig. 10: Stolen Username and password

In this figure, we can see that username and password in the plain text even it can show all the details of the website with a link. Even this can capture the session ID's of the session. This figure shows that SSL Striping our attack successfully was done and stole session ID as well as username and password.

3. Session Hijacking Counter Measures

There are many ways are available for the prevention from session hijacking. But these ways depend on the users how much they are serious about their security. It is said that attacker uses the user's unawareness of about security to steal their important information and sometime attacker make fool to a user and steal the information. According to the CEHv8
Ethical Hacking and counter measure's techniques [9], we are going to divide the countermeasures against session hijacking into two layers from the OSI (Open System Interconnection) mode which is given below:

- Network Layer
- Application Layer

4. Network layer

4.1. Secure socket layer

Always use Secure Socket layer that provides end to end encryption to the data. So whatever data passes through this network secure socket layer it keeps in an encrypted form so it very hard for the attacker to see the exact data passes through the network. Even if an attacker gets the data it is very tough for him to find the real data from the packets. SSL channels use public key 28 bits and symmetric key 256 bits which make the encryptions method more complex, strong and more protected [2].

4.2. Use secure shell (SSH)

Secure shell is also known as Secure Socket shell, this is one of the network protocols which provide the users a secure way to access the remotely situated system or remote computer. This Secure Shell provides the strong way of authentication and more strong way of encryption between two systems in an insecure network also, which help the user to keep the users away from the session hijacking kind of attacks [7].

4.3. Use of HTTPS

This is most important to use the HTTPS (Hyper Text Transfer Protocol Secure) connection whenever we login in any website or any web server or while doing online banking, online shopping or E-commerce. A user should be attentive while all the online related work that URL always should be in HTTPS form because it makes the connection secure and it shows that it is a secure link for online work. If the link is not https form it is insecure and data will traverse in a plain text [3].

5. Application layer

Application layer is the send part of security layer deals with session ID hijacking there some countermeasure which given below.

5.1. Complex and strong session ID

Session ID provides the unique identity to each session as well as user in order to track progress of user and the authentication state of the users in the web application, each application provides the users session identifier that is also known as Session ID or a token, which is assigned to the session when the session is created and used to share with the users and application server in order to track users activities. This session id will be valid till the session is valid once the session gets expired [11].
There are some important steps to be followed in order to make the session id strong and more complex.

5.1.1. Random session ID

Always use a random session ID generation make the attacker very harder to guess the session ID.
Long session ID: If the session ID will be long enough then it provides the good security in order to protect from the brute force attack.

5.1.2. Session ID generated by server

Always use the server generated session ID that makes the session ID more complex and strong because servers user algorithm to generate the session id and it is very tough for the attacker to creak also.

a). **Encrypted session ID**: Encryption is the best way to protect the session ID. Encrypted session ID traverse in the network in an encrypted form which makes it unidentifiable [7].

b). **Automatic log out**: There should be implementation or mechanism to force log out at the particular time and server request to client re-establish the connection with a new session ID. It helps the session and session ID to stay away from the session hijacking and maintain the user's authentication.

6. Conclusion

This paper provides all the information of session hijacking attack and shows how dangerous it is for the network security. Still many peoples are unaware from these kinds of attacks and network security expert also don't take it much seriously and lack of knowledge of session hijacking attack there is still poor session management of some of the web application and web server. In this paper, we have discussed various countermeasures from the session hijacking attack which don't fully prevent the session hijacking attack but it makes the attacker harder to get success on that. There is still needs to do lots of changes in the web applications and server in order to make it permanently finish session hijacking king of attack. This paper mainly focuses on the countermeasure of session hijacking.

References

[1]. Kamal, Parves. "State of the Art Survey on Session Hijacking." *Global Journal of Computer Science and Technology* 16.1 (2016).

[2]. Alabrah, Amerah, and Mostafa Bassiouni. "Preventing session hijacking in collaborative applications with hybrid cache-supported one-way hash chains." *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2014 International Conference on*. IEEE, 2014.

[3]. Jain, Vineeta, Divya Rishi Sahu, and Deepak Singh Tomar. "Session Hijacking: Threat Analysis and Countermeasures." *Int. Conf. on Futuristic Trends in Computational Analysis and Knowledge Management*. 2015.

[4]. Burgers, Willem, Roel Verdult, and Marko Van Eekelen. "Prevent session hijacking by binding the session to the cryptographic network credentials." *Nordic Conference on Secure IT Systems*. Springer, Berlin, Heidelberg, 2013.

[5]. Jha, Saurabh, and Shabir Ali. "Mobile agent based architecture to prevent session hijacking attacks in IEEE 802.11 WLAN." *Computer and Communication Technology (ICCCT), 2014 International Conference on*. IEEE, 2014.

[6]. Sivakorn, Suphannee, Iasonas Polakis, and Angelos D. Keromytis. "The cracked cookie jar: HTTP cookie hijacking and the exposure of private information." *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, 2016.

[7]. Burgers, Willem, Roel Verdult, and Marko Van Eekelen. "Prevent session hijacking by binding the session to the cryptographic network credentials." *Nordic Conference on Secure IT Systems*. Springer, Berlin, Heidelberg, 2013.

[8]. Letsoalo, Enos, and Sunday Ojo. "Survey of Media Access Control address spoofing attacks detection and prevention techniques in wireless networks." *IST-Africa Week Conference, 2016*. IEEE, 2016.

[9]. CEHv8. Ethical Hacking and Counter Measures."Session Hijacking Module 11" [Online]. Available:https://www.wiziq.com/tutorial/714466-CEHv8-Mod ule-11-SessionHijacking. [Accessed: 10-Oct-2014].

[10]. http://searchsoftwarequality.techtarget.com/definition/session-ID