ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. 2, Special Issue I, January 2016 in association with
KARUR VELALAR COLLEGE OF ARTS AND SCIENCE FOR WOMEN, KARUR
Conference on Emerging Trends and Functional Applications of Computer Technology - 12th January 2016

A BRIEF INSIGHT ON SESSION HIJACKING ATTACK, CHALLENGES AND COUNTERMEASURES IN SOCIAL NETWORKS

V.THILAGAVATHI[1]
Research Scholar (Part-Time)
Bharathiyar University
Coimbatore
Tamil Nadu, India.
Thilagavathi.research@gmail.com

Dr. N. NAGADEEPA[2]
Principal
Karur velalar college of arts and science for women
Kuppam(po), karur 639 111, india.
nagadeepa1012@gmail.com

ABSTRACT:
Generally hackers aim is to break the security of computer system, networking system and using this security breach, the intruder steals the valuable things. Session Hijacking is a technique used to break the security of the computing systems. One of the popular incident that exploits session hijacking attack vulnerability is Firesheep – an add one of Firefox browser. Session Hijacking is a form of Man-in-the-middle attacks which are increasingly creating unbelievable impact on all of web based sensitive information transactions. The man-in-the-middle (or middleperson) attack is one in which legitimate parties communicate via a hostile adversary but without their knowledge or consent. This attack can be devastatingly effective because the adversary enjoys complete control of the communication link and can inspect, inject, delay, delete, modify and re-order traffic to suit their purpose. It may be used, for example, to bypass weak authentication protocols, hijack legitimate sessions, perform active traffic analysis and deny service[They are hard to detect but easy to do. It refers to the exploitation of valid computer session to gain authorized access to the information or computer system services. . Session hijacking attack is launched by making fake access point. If we detect the fake access point then we can stop session hijacking, and various techniques had been proposed. In this paper, we are giving a new mechanism to detect the fake access point with the use of sensor nodes in the network. In this paper, session hijacking, its consequences along with the countermeasures is discussed, This paper also shows how the fake access point is used for session hijacking.

Keywords – Session Hijacking, Spoofing, Fake Access Point**,** man-in-the-middle attack, cookies, Wireshark

1 Introduction : The wireless networks can be broadly classified into two categories the Infrastructure and Ad hoc networks. In Infrastructure type of network, central controller is responsible for data routing and controlling the mobile devices. In the infrastructure-based network, communication typically takes place only between the wireless nodes and the access point, but not directly between the wireless nodes. The network attacker s can able to break the security control and illegally access the computing resources. The attackers are either active or passive attackers. Passive attacks does not destroy any computing resources. Their aim is only to steal the valuable information. But active attacks affects the normal behavior of the network. Passive attacks may leads to the active attack. The most common active attacks is the man-in-middle attack, session hijacking attack, denial-of service attack. When user logs into any website, a session with session ID is created on the web server for that user. Basically, sessions contain the entire user’s information. For any page request, the user name and password are not needed. Each user has a unique identifier called as “session ID” or “Session Identifier” to authenticate particular user to the session. This session ID is passed between the web server and the user’s computer system at every message request, reply and vice versa. A session ID is used to manage the session which is called “session token”. Session Hijacking is also called as “Session Side jacking”, is a form of Man in the Middle attack in which a malicious attacker has access to the transport layer and can eavesdrop on communications. When communications are not protected attackers can steal unique session token and impersonate the victim on the target. This allows the permission to the attacker to access the account and data. The state of the session is maintained using cookies. Those Cookies are also used to identify the user. There are three different types of session hijack attacks:

1. Active Session Hijacking
2. Passive Session Hijacking
3. Hybrid Session Hijacking

1.1 Active session hijacking : In active session hijacking, attacker will silence in one of the machines, usually at the client computer, and take over the clients' position in the communication exchange between the workstation and the server. Once the attacker takes the client's position ,they drop the connection between the user and the server. There are various methods for dropping the connection to the server, one of the most common is to send the huge amount of traffic, and this type of attack is known as Denial of Service. By doing this attacker has full control over the session and it communicate with the retending that it is the authenticated user fig1 how a typical session hijacking is conducted a client and a server by an attacker. actual on of the active session hijacking.

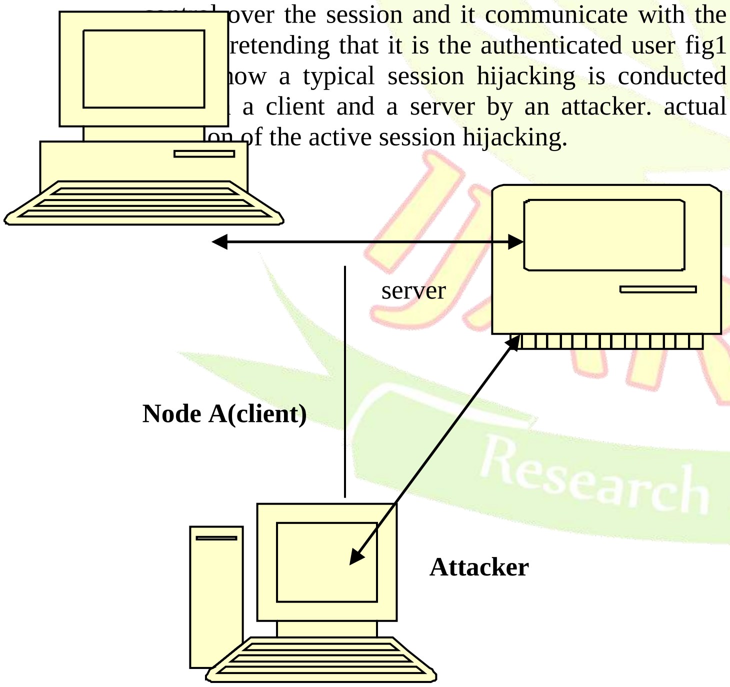

Fig 1. Architecture of active session hijacking

1.2 Passive session hijack :

Passive session hijack attacks are similar to the active attack, but instead dropping the user from the communication session, the attacker monitors the traffic between the workstation and server . In a passive session the attacker listens to all the data and captures them for future attacks, in most cases to perform any type of a hijacking attack it is important that the attacker starts off with passive mode.

1.3 Hybrid Session Hijacking:

Hybrid Session Hijacking is a combination of the active and passive attacks, which allow the attacker to monitor the network traffic until some useful information is found. The attacker can then modify the attack by removing the workstation computer from the session, and assuming their identity. Session Hijacking is widely used to hack the website accounts such as E-mails: Gmail, yahoo, Facebook, twitter, rediff, and online banking transactions widely used for E-commerc etc. In those applications, session ID is stored in the form of cookies in the client's browser and it is used to identify the identity of the user uniquely. To hijack some one's session, we need to steal the session information of that corresponding user.

Session Hijacking can be done at two levels.

1. Network Level
2. Application Level

Network level hijacking is a TCP and UDP session Hijacking and Application level is a HTTP session Hijacking. In application layer, a session ID is obtained through HTTP session hijack. Session Hijacking also known as "Cookie Hijacking". Three types of security services such as authentication, integrity, and confidentiality are provided by securing the Cookies . Therefore it is important to secure Cookies to avoid TCP session hijack attacks. Authentication verifies the cookies owner, Integrity protects against unauthorized modification of cookies, and confidentiality protects against cookies values being revealed to an unauthorized entity.

Sniffing: An attacker uses the sniffer for sniffing a valid session IDs on the network. This technique is used in Wireshark tool. It actually keeps its eye on network traffic and from this utility we can use valid token session to gain authorized access in an unauthorized way.

Session Token Prediction: It is commonly used to predict a session ID of the legal client for accessing the computing session in order to access the valuable information. It actually helps an attacker to exploit compromised user privileges to ping the websites with them.

MITM attack:

The MITM attack stands for Man in the Middle attack.It is used to intercept into an existing connection between machines to know exchanged messages between user and server.
Process: First split the TCP connection into two connection. Client toAttacker and An Attacker to Server. Once the illegal connection is made between attacker and client and attacker and server , an attacker can read, modify and even inject data into this connection.

2 MIB attack :

The MIB attack stands for Man in the Browser attack. It actually makes use of the Trojan horse to intercept the calls between the browser and its security model. It is mainly used for causing financial deceptions by modifying transactions of Net Banking mechanism.

TCP Session Hijacking uses the following five steps.

1 Locating a target that needs to be attacked
2 Finding an active session that wants an attacker to be attacked
3 Observe the capture packet and analyze the stolen cookies and predict the sequence number .
4 Make the user i.e. the victim system to be offline.
5 Attacker takes over the session and maintains the connection

To perform the Session Hijacking: Wireshark, Hamster and Ferret are used

3 Detection of Fake Access Points

The popularity of wireless local area networks (WLANs) increases the risk of wireless security attacks. The fake access points can be deployed in the public places and these access points are kept unencrypted. Fake access point is created anywhere in public like hospitals, colleges, airports etc. When the access points are unencrypted and maximum legitimate users will try to connect with that. When legitimate users connect to the fake access point, attack gathers the information. The various techniques are used to detect the fake access points..

4 Countermeasures: When the people access the network, they should aware of set of countermeasures used for the session hijacking.

1. Use SSL to have secure communication channel.
2. There must be logout function for session termination.
3. Trust HTTPS connection for passing authentication cookies.
4. Always pass encrypted data between user and webservers.
5. Adopt a secure protocol.
6. Regeneration of Session ID after log in.
7. Reduce having remote access.
8. Emphasis on Encryption.
9. Reduce incoming connections.
10. Reduce the life span of session or cookie. Always create session keys with lengthy strings or random numbers.
11. Try preventing Eavesdropping.
12. Expire the session as soon as user logs out.
13. Do not access links received through mails.
14. Use firewall and browser settings to restrict cookies.
15. Make sure website which we are accessing is certified by certified authority.
16. Clear history, offline contents and cookies from browser after every secret or sensitive transaction.

5 CONCLUSION

The hijacking a TCP session is successfully done at network and application levels of reference layers by hijacking a TCP session and stealing cookies. Securing websites against Session hijacking attacks are done by some techniques such as securing the cookie generation, implementing Confidentiality, Integrity, Authentication etc. Session hijacking is active type attack and it has very bad impact on the network .The fake access points will work like honey pot and used to gather network information. If the fake access points are detected which will work like a honey pot then session hijacking will be prevented .

REFERENCES

[1] Internet Crime Complaint Centre link: www.ic3.gov

[2] Liu, Bingchang; Shi, Liang; Cai, Zhuhua; Li, Min; “Software vunerability Discovery Techniques : A Survey” IEEE Conference Publication, DOI : 10.1109/MINES.2012.202, Page(s) 152-156, 2012

[3] Smith, Yurick, Doss “Ethical Hacking” IEEE Conference Publication, DOI: 10.1147/sj.403.0769, Page(s): 769-780

[4] Bradley, Rubin “Computer Security Education and Research: Handle with care” IEEE Conference Publication, DOI : 10.1109/MSP.2006.146, Page(s): 56-59

[5] Wilbanks “When Black Hats are really white” IEEE Conference Publication, DOI:10.1109/MITP.2008.146, Page(s): 64

[6] Shray Kapoor, “Session Hijacking Exploiting TCP, UDP and HTTP Sessions”, Information Security Writers Commercial site text resource.

[7] Chris Sanders, “Understanding Man-In-The-Middle-Attack – Part 3: Session Hijacking”, Articles and tutorials published on 5th May 2010, WindowSecurity.com affiliated with Microsoft Corp.

[8] ISTR, “Internet Security Threat Report 2014”, Symantec Corporation, 2013 Trends, Volume 19, p. 87, Published April 2014.

[9] Jerry Louis, “Detection of Session Hijacking” University of Bedfordshire Repository, Department of Computer Science and Technology, Supervisor: Dr. Xiaohua Feng, 10547/211810, AY10/11, January 2011.

[10] Nadeem A Kayani, “Security Test Tools”, Open Source Testing Organization: Open Source Software Testing Tools, News and Discussion Testing tools - Security.http://www.opensourcetesting.org/security.php Or Wireshark foundation, https://www.wireshark.org/

[11] Kevin Lam, David LeBlanc, and Ben Smith “Theft On The Web: Prevent Session Hijacking“ TechNet Magazine, Issues 2005 Winter, Chapter 21 of Assessing Network Security (Microsoft Press, 2004).

[12] Joon S.Park and Ravi Sandhu, “Secure Cookies on the Web” IEEE Internet Computing 4 (2000), 36-44.

[13] Italo Dacosta, Saurabh Chakradeo, Mustaque