A Survey on Detection Tools and Prevention Techniques for Session Hijacking Attack

D.Madhavi[1]
[1]Assistant Professor
[1]V.R.Siddhartha Engineering College, Vijayawada, A.P., India

Abstract— Session Hijacking is the process of accessing the session by stealing session ID or Cookies. In session hijacking attack, unauthorized person can impersonate one of the sessions of a victim and takes control over it like a legitimate user. It is a one of the most dangerous attack performed on transactions done over a network like E-commerce, which handles the confidential or sensitive information over a web. There is no other way to avoid this attack, unless until first need to detect and then prevent it. This paper examines the closer look at the detection tools and prevention techniques that are used to prevent the session hijacking attack.

Key words: Session hijacking attack, session hijacking detection tools, session hijacking prevention

I. INTRODUCTION

Now a days, the usage of web based applications are increasing and the session vulnerabilities are very common in all web applications. Attackers are taking an advantage of poorly configured websites to hijack user's sessions and take control over their identity. An important piece of information is stored on the session state. For this reason session state represents a valuable target for the attackers. Attackers can steal; replace a user's session by masquerading like actual user. Therefore session management [9] is the important web application security risk. Session state maintains an important role in maintaining a secure session management. A Session State includes the session ID, session timeout, session mode, session key, session type (private/shared), cookie, user data, is session read-only, is session safe, etc. User must need to pose the security concepts to Session Management [13] [14].

There are different types of sessions such as active session, passive session and hybrid sessions. Whatever be the type of the session, the session hijacking can be performed by an attacker. Generally, Session Hijacking is a passive attack. If this is the case then it is difficult to detect session hijacking attacks [1]. Victim cannot be able to detect this attack until unless attacker performs some obvious action on the current session. Victim does not know what an attacker did there. Therefore some of the tools are used in detecting whether the session has hijacked or not, which are discussed in the following section. Some of the tools used in session hijacking are Hunt, T-Sight, Juggernaut, TTY Watcher, Hamster and Ferret, Wireshark, Ethereal and many more [1][2].

The defending mechanisms on session hijacking is very important for all the web based applications, transactions over web which of those handling sensitive information, business operations, E-Commerce transactions. The mechanisms are discussed in the following concepts of this paper.

II. DESCRIPTION

There are so many scientists are designing and developing different detection tools for different attacks and different prevention techniques for remediation of session hijacking. Some of the Detection Tools and Techniques for Session hijacking [2] are Arp-ON, ARP-PING, ANTI-SNIFF, Cookie Monster, Wavelet Based Detection, Cisco Intrusion Detection System (IDS), and Sans Intrusion Prevention System (IPS) are shown in the Table I.

There are some algorithms and Techniques for preventing Session Hijacking [2], they are

(1) Ensuring a secure Cookie generation
(2) Implementing the CIA technology, C-Confidentiality, I-Integrity, A-Authentication.
(3) Use encrypted connections or protocols for the transmission of data such as HTTPS, Open SSH protocol suite.
(4) Locking a particular session to its corresponding user's i.e. Session Lock [15].

Tool Name	Author Name & Year	Tool Function	Type of Attack to Avoid
Arp-ON	Darknet, 2000	To secure the Address resolution Protocol	MITM (Man-In-The-Middle) attacks
ARP-PING	Beyond-Security, 1998	Allows the user to ping MAC address directly	To detect Sniffer on the network
ANTI-SNIFF	Storm, 2011	Used for Packet Capturing	Packet Sniffer
Cookie-Monster	Pauli, Engebretson, Ham &Zautke, 2011	Analyzing the strength of the cookie by archiving & analyzing	Cookie stealing
Wavelet-Based-Detection	Long &Sikdar, 2008	Analysis the signal strength using Wavelet Transform	Session Hijacking

Table 1: Session Hijacking Detection Tools

A. Ensuring a Secure Cookie Generation:

Cookie is the one important component in web based applications, which can be used to authenticate a client and cookie information is sent to the server system for that user. The cookie information contains user name, password, timestamp, session timeout. Whenever a session is hijacked, the attacker analyses this cookie information and comprises the user's account.

B. Implementing the CIA Technology:

This is the low cost solution to secure session cookies. This also prevents cross-site-scripting. This is achieved by creating a java script on the server side and cookie is available only to the client's browser. It develops the standard plug-in for the Chrome, Mozilla Firefox, etc.

C. Use Encrypted Connections For The Transmission:

The connection was encrypted with HTTPS (Secure Hyper Text Transfer Protocol) and this protocol uses a SSL (Secure Socket Layer) protocol stack. The drawback is cost. Implementing and maintaining this service is cost effective.

D. Locking a Particular Session:

This is an effective technique to prevent session hijacking. Even if the session is hijacked, the attacker has no use. A unique HMAC (Hashed Message Authentication Code) algorithm with secret key is shared between client and server. A token is generated from an initial login over the SSL. This is an efficient and low cost solution to secure the session.

These are the most common widely used ways to prevent the session hijacking attacks. Not only had these some of the methods are used to prevent session hijacking are using Encryption, re-authentication, session timeouts [11], SHPF (session Hijacking Prevention Framework) [16], Fake access points and IP spoofing [17]. Some of the security tools [11], Network Sniffers, Vulnerability Scanners are used to detect the session hijacking.

Researcher Name	Year	Proposed Method for Detection	Procedure
Long and Sikdar	2008	Algorithm to detect Session hijacking in Wireless networks	Based on detecting colored noise in the received signal strength during the attack
Louis [2]	2011	Dual approach in using both an IN-Network Strategy and OUT-Network Strategy	OUT-Network has more control on detection of Session Hijack from outside network. Whereas IN-Network has more efficiency on LINUX system for detecting an attack inside the network. Detection rate is 65%.
Nikiforakis et al.	2011	Light Weight Client-Side Detection Mechanism Called "Session Shield"	Based on the idea of Session ID's. Session Shield detects ID from incoming HTTP traffic and isolates them from web browser. This way session ID's are protected from all evil scripts.

Table 2: Session Hijacking Detection Methods

Different researchers proposed different techniques to prevent session hijacking [5]. Different session hijacking detection methods are shown in the Table II.

Prevention Technique for Nikiforakis's technique is generates a random session ID with a long string called a session shield. Many of the researchers give solutions to the prevention of session hijacking are shown in below table III.

Author	Year	Prevention Technique
Nikiforakis et al. [10]	2011	Session shield
Dacosta et al. [7] [8]	2011	OTC (One-Time Cookies)
Asif&Tripathi [12]	2012	Double authentication to User ID

Table 3: Prevention Techniques

By using of these techniques the research people mitigate the risk caused by the session hijacking in an open ID network environment. Different researchers produce different detection and prevention techniques for different attacks [5] [14] such as session fixation, Cross Site Request Forgery (CSRF), replay attacks and many more in both wired and wireless open networks. Different types of losses are occurred due to different attacks and amount of loss is almost immeasurable. The types of losses vary from user to user and application to application in an open network. The classifications of losses are as follows:

- Communication data or information loss
- Leakage of information
- Spam and Worm penetration in applications
- Planting of malware
- Credit card details leakage
- Spreading of disinformation
- Loss of sales
- Information conflicts at war
- Website impairment
- Machines or applications downtime
- Link spam
- Pecuniary loss

E. Against Session Hijacking:

Using SSL and HTTPS does not provide the full security i.e sslstrip [18] is used to stripping "*https://*" to *"http://"* URL. But HSTS (HTTP Strict Transport Security) is a solution to this problem. To better care about sensitive transaction data use and save online transactions at home, secure machines by using Firewalls, Proxies and Gateways [4][11] which are developed by various infrastructures giants like Cisco, Juniper, etc. Performing online transactions at "home" is more secure than office. This result the chances of somebody watching network traffic are very low. Basically a session based operations done on a device can be able to determine that somebody is watching in shadow. Therefore keep an eye out for things and pay attention to "Last log in time", secure internal user's machine, companies must provide VPN (Virtual Private Networks) to users when they are away from the office, if the network is wireless then use WPA (Wireless Protected Access) encryption.

In Wireless LAN, a Honeypot is used to identify fake access points for preventing session hijacking [3][6]. But this technique has the vulnerability of MAC Spoofing

which is prevented by the use of public private key cryptography.

III. CONCLUSION

The session hijacking cannot be able to mitigate until unless if the attacker detects it. Therefore this paper gives a brief summary about various researchers' work on detection and prevention techniques on session hijacking. If it is not the case of defending the session hijacking attacks then victim can be the side of a big loss in case of E-Commerce and large business related organizations. Some of the session prevention techniques are costlier but some of them are cheaper and efficient. The victim must be follow any of the prevention techniques based on their applications with respect to either it is wired or wireless networks.

REFERENCES

[1] D.Madhavi, TCP Session Hijacking Implementation by Stealing Cookies. International Journal for Scientific Research and Development, Volume 2, Issue 11, Jan (2015): 300-303. http://www.ijsrd.com/articles/IJSRDV2I11175.pdf

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

[3] Abhishek Kumar Bharti, ManojChaudhary, Detection of Session Hijacking and IP Spoofing Using Sensor Nodes and Cryptography. IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727 Volume 13, Issue 2 (Jul. – Aug. 2013), PP 66-73.

[4] Paul Jess, Session Hijacking in Windows Networks. GSEC Gold Certification, SANS Institute InfoSec Reading Room, White Paper 2124. Practical Assignment Date Submitted: October 12th, 2006. © SANS Institute 2008.

[5] BijuIssac, NaumanIsrar, Case Studies in Secure Computing: Achievements and Trends. Chapter 17, Session Prediction/Hijacking, CRC Press: Taylor & Francis Group, LLC, An Auer Bach Book. © 2015, ISBN- 13:978-1-4822-0707-1 (eBook).

[6] Rupinder Gill, Jason Smith, Andrew Clark, Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks. 4th Conferences in Research and Practice in Information Technology, (Network Security), AISW 2006, Hobart, Australia. ACS 221-230. http://crpit.com/abstracts/CRPITV54Gill.html

[7] DacostaItalo, SaurabhChakradeo, MustaqueAhamad and Patrick Traynor, One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens. ACM Transactions on Internet Technology (TOIT), Volume 12, Issue 1, Article No. 1, doi> 10.1145/220352.2220353, June 2012.

[8] DacostaItalo, SaurabhChakradeo, MustaqueAhamad and Patrick Traynor, One-Time Cookies: Preventing Session Hijacking Attacks with Disposable Credentials. SMART Tech Scholarly Materials and Research at Technology, Georgia Tech Library. SCS Technical Report; GT-CS-11-04, 2011. https://smartech.gatech.edu/bitstream/handle/1853/37000/GT-CS-11-04.pdf?sequence=1.

[9] Umesh Kumar Singh, RakhiSunhare, Kailash Chandra Phuleriya, Study and Analysis of Session Security on Web Based Applications. International Journal of Advanced Research in Computer Science and Software Engineering, Research Paper, ISSN: 2277 128X, Volume 3, Issue 12, December 2013. http://www.ijarcsse.com/docs/papers/Volume_3/12_December2013/V3I11-0634.pdf

[10] Nick Nikiforakis, WannesMeert, Yves Younan, Martin Johns, WouterJoosen, Session Shield: Lightweight protection against session hijacking.ACM Digital Library, ESSoS'11 Proceedings of the 3rd international conference on Engineering secure software and systems, pages 87-100, ISBN: 978-3-642-19124-4, Springer-Verlag Berlin, Heidelberg © 2011.

[11] Abdullah H. Alqahtani, MohsinIftikhar, TCP/IP Attacks, Defenses and Security Tools. International Journal of Science and Modern Engineering (IJISME), ISSN: 2319-6386, Volume-1, Issue-10, September 2013.

[12] Asif Muhammad, NitinTripathi, Evaluation of Open ID-Based Double-Factor Authentication for Preventing Session Hijacking in Web Applications. Journal of computers, Academy Publisher, Volume 7, No 11, doi>10.4304/jcp.7.11.2623-2628, Nov 2012. http://ojs.academypublisher.com/index.php/jcp/article/view/jcp071126232628/5787

[13] Gunter Ollmann, Web Based Session Management: Best practices in managing HTTP-based client sessions. TECHNICAL INFO: Making sense of security, White papers. http://www.technicalinfo.net/papers/WebBasedSessionManagement.html

[14] Luke Murphey, Secure Session Management: Preventing SecurityVoids in Web Applications. SANS Institute InfoSec Reading Room, GSEC Practical 1.4c, option 1, Revision Number 3, January 10, 2005.

[15] Ben Adida, Session Lock: Securing Web Sessions against Eavesdropping. ACM Proceedings, 17th International conference on World Wide Web, New York, NY, USA, ISBN: 978-1-60558-085-2, doi>10.1145/1367497.1367568,pages 517-524, April 2008.

[16] Thomas Unger, Martin Mulazzani, DominikFruhwirt, SHPF (session Hijacking Prevention Framework): Enhancing HTTP(S) Session Security with Browser Finger Printing (Extended Preprint). IEEE 8th International Conference on ARES (Availability, Reliability and Security), pages 255-261, doi>10.1109/ARES.2013.33, 2013.

[17] Abhishek Kumar Bharti, ManojChaudhary, Prevention of Session Hijacking and IP Spoofing

with Sensor Nodes and Cryptographic Approach. International Journal of Computer Applications (0975 - 8887), Volume 76, No. 9, August 2013. http://research.ijcaonline.org/volume76/number9/pxc3890821.pdf

[18] FenilKavathia, Ajay Modi, SSL Enhancement. International Journal of Computer Applications (IJCA) Special Issuse on "Network Security and Cryptography", NSC, Number 3, SPE029T, 2011. http://research.ijcaonline.org/nsc/number3/SPE029T.pdf

