ISSN No. 0976-5697

Volume 4, No. 9, July-August 2013

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review on Detection of Session Hijacking and Ip Spoofing

Abhishek Kumar Bharti, Maggi Goyal
Student, Computer Science Department
YCoE , Punjabi University
Bathinda
abhiarch21.bharti@gmail.com, agg.maggi@gmail.com

Manoj Chaudhary
Assistant Professor, Computer Science
YCoE , Punjabi University
Bathinda
ermanojchaudhary@gmail.com

Abstract - In today's world the computer networks where the packets are sent over the network form client to server for getting the services and server to client to provide the services. As the packets are moving in the network there are vulnerable to numerous types of attacks can be done on the packets . Either it is wireless network or wired network, one of the most common attacks is man-in-the-middle attack, in which session hijacking and IP spoofing has been the most attempted attack. As compare to other attacks the success rate of a session hijacking and IP spoofing attack is higher. Earlier studies on detection of session hijacking and IP spoofing is based on the IN and OUT strategy of the session hijacking. This paper serves some of the detection algorithm for detecting the Session Hijacking and IP spoofing along with the current proposed solutions. And the platform it uses for the study are Windows and Linux.

Keywords: Session Hijacking, IP spoofing, Man-in-the-middle-attacks.

I. INTRODUCTION

In the age of communication everything happens on the internet form business to shopping, from banking to education internet important plays a very important role. And As the internet grows larger and larger the security threat has grown even more strongly. Security plays a major role in every aspect of communication or transaction over any network. Every user out there needs to be assured that their information, money, transaction and communication are safe and trustable with the related network they are engaged in[8]. There are various security threats that cover on the internet starting form man-in-middle attack, Denial-of-Service attack, Distributed-Denial-of-Service attack, IP spoofing etc. So it has become a tedious task for every system administrator and computer security professional to be competent enough of to develop various defensive mechanisms to handle uncertain attacks and protect the user information. This paper aims to address the most effective security attacks known as Session Hijacking and IP spoofing.

A. Session Attack:

A typical session hijacking is a well known man-in-middle attack in the world of network security and its one of the favorite attack for the attackers because of the nature of the attack. A user who is already logged in (authenticated) to a web server and has a valid session existing between the user and the server, the attacker takes control over such a session, basically hijack the session from the user and continues the connection to the server pretending to be the user. As the user is already authenticated so attacker need not to waste hours for cracking the password. There are three types of Session Hijacking attacks:

a) Active Session Hijacking
b) Passive Session Hijacking
c) Hybrid Session Hijacking

a. Active Session Hijacking:

An active session hijacking is one in which the attacker takes control over an active session of the victim and starts to pretend as a genuine user by communicating to the server. There are several methods to drop a user's connection to the server, one of the most common is to flood the target machine with huge amount of traffic, and this type of attack is known as Denial of Service. By doing this the attacker puts the user into offline mode, now the attacker has full control over the session. Throughout this process the attacker is in stealth mode listening and monitoring the packets traversing over the network[8].

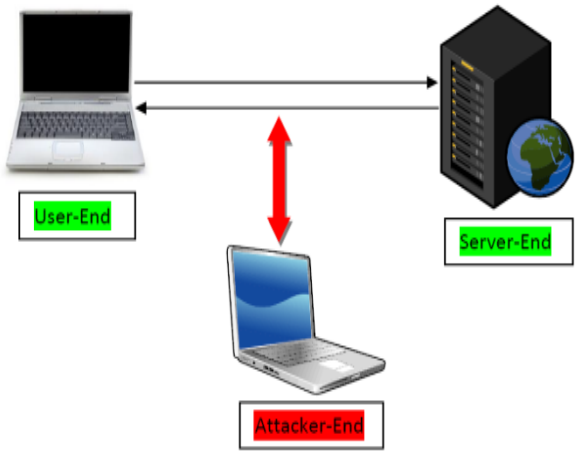

Figure: 1 Active Session Hijacking[8]

As illustrated in the fig1, it clearly shows how a typical session hijacking attack is conducted between a client and a server by an attacker. The traffic is constantly monitored using the packet capturing tool and then the packets are analyzed to understand which packet contains the session information required to authenticate to server.

b. Passive Session Hijacking:

In a passive session the attacker listen 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. The disadvantage in the passive mode attack is that the attacker might not be that efficient in succeeding on the user impersonating to the server, unless the user session is still alive in most cases it will not be, if the user logs off form the server.

c. Hybrid Session Hijacking:

In hybrid session hijacking the attacker implements both the modes of attacks that is passive and active mode to successfully complete the attacks. In this type of attacks the attacker monitors the pattern of traffic that has been sent over the network and the attacker choose a session to impersonate. All the attacker has to do in this situation is to wait for the right session and hijack the session form the user.

B. IP Address Spoofing:

IP address spoofing is the creation of IP packets using somebody else's IP source addresses. This technique is used for obvious reasons and is employed in several of the attacks . Examining the IP header, we can see that the first 12 bytes contain various information about the packet. The next 8 bytes, however, contains the source and destination IP addresses. Using one of several tools, an attacker can easily modify these addresses – specifically the "source address" field.

A common misconception is that "IP spoofing" can be used to hide our IP address while surfing the Internet, chatting on-line, sending e-mail, and so forth. This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection. When the workstation requests a page from the web server the request contains both the workstation's IP address (i.e. source IP address 192.168.0.5) and the address of the web server executing the request (i.e. destination IP address 10.0.0.23). The web server returns the web page using the source IP address specified in the request as the destination IP address, 192.168.0.5 and its own IP address as the source IP address, 10.0.0.23.

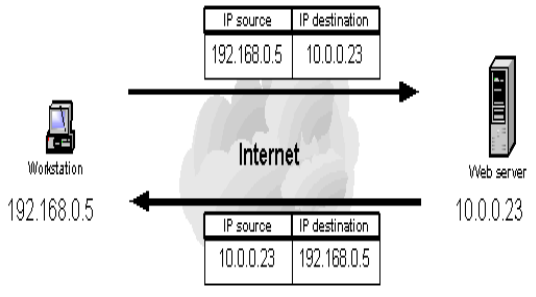

Figure 2: Valid source IP address

Figure 3: Spoofed source IP address, illustrates the interaction between a workstation requesting web pages using a spoofed source IP address and the web server executing the requests. If a spoofed source IP address (i.e. 172.16.0.6) is used by the workstation, the web server executing the web page request will attempt to execute the request by sending information to the IP address of what it believes to be the originating system (i.e. the workstation at 172.16.0.6). The system at the spoofed IP address will receive unsolicited connection attempts from the web server that it will simply discard.

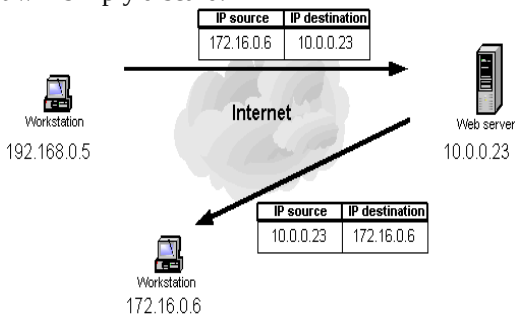

Figure 3 Spoofed IP address

II. RELATED WORK

Session hijacking is the stealing of the session of the user that is use to communicate with the server. In session hijacking a user who is already logged in (authenticated) to a web server and has a valid session existing between the user and the server, the attacker takes control over such a session, basically hijack the session from the user and continues the connection to the server pretending to be the user. And IP spoofing is the creation of IP packets using somebody else's IP source addresses. So in order to detect the session hijacking and IP spoofing various algorithms has been develop Extant defensive techniques and procedures are not completely effective against such attacks. The authors found that some 48% of Indonesian websites are vulnerable to such attacks because, contrary to best software engineering practices, many use default session management IDs generated by their development platforms [6].In year 2012 an ant-based traceback is proposed to detect the IP spoofing. The proposed traceback approach uses flow level information to identify the spoofing request. To validate the detection method further, this paper considers the number of hop needs to reach the destination end. Using a mapping between IP addresses and their flow level with hop-counts, the server can distinguish spoofed IP packets from legitimate ones. The simulations results show that this approach discards almost 90% of spoofed IP request[4].

Rupinder Gill, Jason Smith, Mark Looi and Andrew Clark proposed Passive Techniques for Detecting Session Hijacking Attacks in IEEE 802.11 Wireless Networks in year 2005 two techniques that can be used by a WIDS to passively detect session hijacking attacks. The techniques described meet many of the desirable characteristics proposed as they: are based on unspoofable characteristics of the PHY and MAC layers of the IEEE 802.11 standard; are passive and do not require modifications to the standard, wireless card drivers, operating system or client software; are computationally inexpensive; and do not interfere with live traffic or network performance[3].

Then Gill, Rupinder and Smith, Jason and Clark, Andrew proposed an algorithm that is based on IEEE 802.11 Network to detect the Session Hijacking distinct test scenarios. A correlation engine has also been introduced to maintain the false positives and false negatives at a manageable level. We also explore the process of selecting optimum thresholds for both detection techniques[3]. In year 2009 Al-Sammarraie Hosam ,Adli Mustafa and Shakeel Ahmad proposed an algorithm for IP spoofing over online

environment IP and email spoofing gained much importance for security concerns due to the current changes in manipulating the system performance in different online environments. Intrusion Detection System (IDS) has been used to secure these environments for sharing their data over network and host based IDS approaches[2]. However, the rapid growth of intrusion events over Internet and local area network become responsible for the distribution of different threats and vulnerabilities in the computing systems. The current signature `detection approach used by IDS, detects unclear actions based on analyzing and describing the action patterns such as time, text, password etc and has been faced difficulties in updating information, detect unknown novel attacks, maintenance of an IDS which is necessarily connected with analyzing and patching of security holes, and the lack of information on user privileges and attack signature structure. Thus, proposes an EADS (Exception agent detection system) for securing the header information carried by IP over online environments. The study mainly concerns with the deployment of new technique for detecting and eliminating the unknown threats attacks during the data sharing over online environments[2].

Then In year 2012 Srikanth Kamuni, S.ShreehaTejaswini, Bhaskar.J proposed a technique for detecting the session hijacking based on wavelet based real time session hijack detection based on Bluetooth signal analysis in which it tells A session hijacking is predominantly a man in the middle attack for wireless network where the attacker places itself in the route between the source and the destination node such that all the traffic is routed through the malicious node[1]. A session hijacking is the result of accidental association attack or MAC spoofing attack. In this case the attacker places itself close to either the source or the destination or any other router node in such a way that it is considered as a legitimate router node. Therefore detection rate in most of the existing technique is low and unreliable. In this work we propose a real time mechanism for detecting the session hijacking attack by analyzing the signals received from the nodes through a monitoring station in the wavelet domain. We first setup a 802.11 based network with the help of Bluetooth without any authorization. i.e. the nodes can communicate with exchanging any keys. We use a monitoring station where we use an Arduino board to capture the amplitude variation of the Bluetooth receiver.. First we analyze the signal in the wavelet domain when only two nodes are exchanging constant bit rate traffic. Further wireless Packet injection is implemented with another device and the signal patterns are analyzed by signal analyzer. Significant conclusive structures are extracted. These signatures are further used to classify the online data at every predefined interval of time[1].

III. COMPARITIVE STUDY

Author(s)	Year	Paper Name	Technique	Result
Srikanth Kamuni, S.ShreehaTejaswini, Bhaskar.J, Dr. G.Manjunath [1]	2012	Wavelet Based Real Time Session Hijack Detection Based On Bluetooth Signal Analysis	Monitering System using bluetooth	Efficiency increased to 90 % And its real implemented and can be applied to wifi and other networks.
Al-Sammarraie Hosam and Adli Mustafa[2]	2009	Exception Agent Detection System for IP Spoofing Over Online Environments	Create an intrusion detection system for ip spoofing	More efficient but costly.
Rupinder Gill, Jason Smith, and Andrew Clark[3]	2006	Passive Techniques for Detecting Session Hijacking Attacks in IEEE 802.11 Wireless Networks	Passive technique	Can detect the session hijacking but selecting a threshold that is too high will lead to false negatives.
N.Arumugam, Dr.C.Venkatesh[4]	2012	A Dynamic Method to Detect IP Spoofing on Data Network Using Ant Algorithm	ant-based traceback	Ensure good filtering of packets
Noureldien A. Noureldien, Mashair O. Hussein[5]	2012	Block Spoofed Packets at Source (BSPS): A method for Detecting and Preventing All Types of Spoofed Source IP Packets and SYN Flooding Packets at Source	Network authentication server	By network ad-ministrators and ISP's to alleviate bogus traffic in the Internet.
Bhavna C.K. Nathani Erwin Adi [6]	2012	Website Vulnerability to Session Fixation Attacks	identifying vulnerable websites	Can protect form session identifier but not for legitimate client-side scripts
Mrs. Mridu Sahu and Rainey C. Lal[7]	2012	Controlling IP spoofing through packet filtering	Packet filtering	Preventing spoofing through Packet filtering
Thawatchai Chomsiri[9]	2008	A Comparative Study of Security Level of Hotmail, Gmail and Yahoo Mail by Using Session Hijacking Hacking Test	Anlysis of Hotmail, Gmail and Yahoo	Yahoo has the maximum security then hotmail and gmail.

IV. CONCLUSION

In this comparative study of session hijacking and IP spoofing and find that most common active attack is session hijacking that can be attacked at the server, client and in between the server and client. Various techniques have been studied to detect and prevent the session hijacking and IP spoofing each technique has their own advantages and limitations. In Session Shield technique can protect form session identifier but not for legitimate client-side scripts and in Passive technique can detect the session hijacking but selecting a threshold that is too high will lead to false negatives and the failure to detect attacks. In the active and

passive host-based methods it tells the session hijacking and IP spoofing. So passive host based methods is preferred to detect the IP spoofing.

V. REFERENCES

[1]. Srikanth Kamuni, S.ShreehaTejaswini, Bhaskar.J, Dr. G.Manjunath "Wavelet Based Real Time Session Hijack Detection Based On Bluetooth Signal Analysis" ISSN: 2249-1945 Srikanth Kamuni et al, GJCAT, Vol 2 (2), 2012, 1210-1213.

[2]. Al-Sammarraie Hosam and Adli Mustafa "Exception Agent Detection System for IP Spoofing Over Online Environments" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009.

[3]. Rupinder Gill ,Jason Smith ,Andrew Clark "Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks" Australasian Information Security Workshop (Network Security), 16-19 January 2006, Hobart, Tasmania.

[4]. N.Arumugam, Dr.C.Venkatesh " A Dynamic Method to Detect IP Spoofing on Data Network Using Ant Algorithm" IOSR Journal of Engineering (IOSRJEN) e-ISSN: 2250-3021, p-ISSN: 2278-8719, Volume 2, Issue 10 (October 2012), PP 09-16

[5]. Noureldien A. Noureldien, Mashair O. Hussein "Block Spoofed Packets at Source (BSPS): A method for Detecting and Preventing All Types of Spoofed Source IP Packets and SYN Flooding Packets at Source" International Journal of Networks and Communications 2012, 2(3): 33-37 DOI: 10.5923/j.ijnc.20120203.03.

[6]. Bhavna C.K. Nathani Erwin Adi "Website Vulnerability to Session Fixation Attacks " Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.7, 2012.

[7]. Mrs. Mridu Sahu and Rainey C. Lal " CONTROLLING IP SPOOFING THROUGH PACKET FILTERING" Int.J.Computer Techology & Applications,Vol 3 (1),155-159 IJCTA | JAN-FEB 2012 Available online@www.ijcta.com 155 ISSN:2229-6093

[8]. Jerry Louis "Detection of Session Hijacking" university of Bedfordshire January 2011 page no. – 12.

[9]. Thawatchai Chomsiri "A Comparative Study of Security Level of Hotmail, Gmail and Yahoo Mail by Using Session Hijacking Hacking Test" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008.