INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Detection of Fake Access Point to Prevent Session Hijacking

Hemanshu Kamboj[1], Gurpreet Singh[2]

Lovely Professional University
Jalandhar, Punjab
hemanshukamboj11@gmailcom, gurpreet.16523@lpu.co.in

Abstract: *The wireless network is much vulnerable to security attacks as compared to wired network. In wireless networks we use radio waves for communication. The various types of active and passive attacks are possible. The man-in-middle, session hijacking is the most common active attacks. The session hijacking attack can be generally performed using honey pot. In our work, fake access point is the honey. In the session hijacking attack we attract legitimate user to connect with the unencrypted access point .When the legitimate user connect with the access point, we hack the cookies, sessions of the legitimate user. In this paper, we are proposing new hybrid technique to detect fake access point. Our new proposing technique will be based on the number beacon frames received in fixed time according to the climate conditions .In our work, we also include the type of access from where we are receiving beacon frames.*

Keywords: *Fake access Point, Honey Pot, Beacon Frames, Session, Hijacking, Cookies*

1. INTRODUCTION

The wireless networks can be broadly classified as Infrastructure and Ad hoc networks. In Infrastructure type of network central controller is present which 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 access point does not just control medium access, but also acts as a bridge to other to wireless or wired networks. The base stations are fixed as the node goes out of the range of a base station; it gets into the range of another base station[7]. The ad hoc network is the self configuring type of network in which no central controller is present. Ad-hoc wireless network do not need any infrastructure to work. Each node can communicate directly with other node so no access point controlling medium access is necessary. Infrastructure less networks, do not have fixed routers all the nodes in the network need to act as routers and all nodes are capable of movement and can be connected dynamically in an arbitrary manner.. Figure shows a simple ad-hoc network with three nodes. The outermost nodes are not within transmitter range of each other. However the middle node can be used to forward packets between the outer most nodes. The middle node is acting as a router and the three nodes have formed an ad-hoc network. The various types of active and passive attacks are possible in wireless networks. The passive attacks are those attacks in which attacks don't effect normal behavior of the network and simply sniff the network. In active attacks, attacker affects the normal behavior of the network .Passive attacks may leads to the active attack. The most common active attacks are man-in-middle attack, session hijacking attack, denial-of-service attack. In our work is to prevent session hijacking attack. The session hijacking attack can be

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

generally performed by using honey pots. The fake access point is the honey pot in our work. The legitimate user can connect to the unencrypted fake access point and when legitimate user accesses the services of the access point, attacker can hijack the session, cookies of the legitimate users. 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 hijacks the session from the user and continues the connection to the server pretending to be the user. This has become increasingly common because the attackers are in a great advantage of not having to waste hours and hours to crack a password, or to try and conduct a dictionary attack against the server, since the user has already been authenticated and in a active session it makes it so much easier to just listen to the traffic on the network without the knowledge of the user. When attacker can get the session of the legitimate user, attacker can access the services from the web server on the behalf of the legitimate user.

In this paper, Literature Review is present in the section 2. Problem Formulation is written in section 3. New proposed technique will be discussed in the section 4. In the last section 5 future work and conclusion is presented.

2. Literature Review

The users on the network are increasing drastically from last few years. The wireless networks are used now a days and it is much vulnerable to security attacks. The honey pots are used to perform session hijacking attack. The honey pots are used to monitoring and surveillance and gathering information and understanding the properties of the network. In this paper authors showed a survey results .In this survey for the 4 months honey pots are deployed in the area and different attacks came from the different countries and perform different type of attacks on the network. All the attackers will try to hack the secure SSL server by gathering the information using honey pots [1].

In this paper author proposed a method to detect the session hijacking attack. The proposed will detect the fake access point .The proposed scheme will be based on using wavelet based analysis of the received signal strength. In this technique they developed a model which describes the changes in the received signal strength of the access point. In this technique they used an optimal filter to analyze the received signal strength [2].

In this paper author shows an experimental results about the security levels of the three most secure web mails-Hotmail, Gmail and Yahoo mail. The servers of these three web mails are hacked with session hijacking. The attacker can hack sessions and cookies in LAN system. Attacker can use two methods for session hijacking .The comparison results shows that yahoo mail is highly secure, and then hotmail and Gmail is the least secure web mail [3].

In this paper, authors explained that cross-site scripting is most vulnerable to security attacks in web applications. The most common attack in cross-site scripting is the session hijacking. The session hijacking attack is the client side attack. The attacker can hack the session id through the session ID session will be hijacked. When the session is hijacked the web server will be compromised. In this paper, they proposed a new technique to prevent session hijacking. In this new technique they develop session shield to prevent client sided session hijacking attack. Session Shield is based on the observation that session identifier values are not used by legitimate client-side scripts and, thus, need not to be available to the scripting languages running in the browser. Our system requires no training period and imposes negligible overhead to the browser, therefore, making it ideal for desktop and mobile systems [4].

The wireless networks are gaining popularity day by day. The growing popularity of wireless local area networks (WLANs) increases the risk of wireless security attacks. The fake access points can be

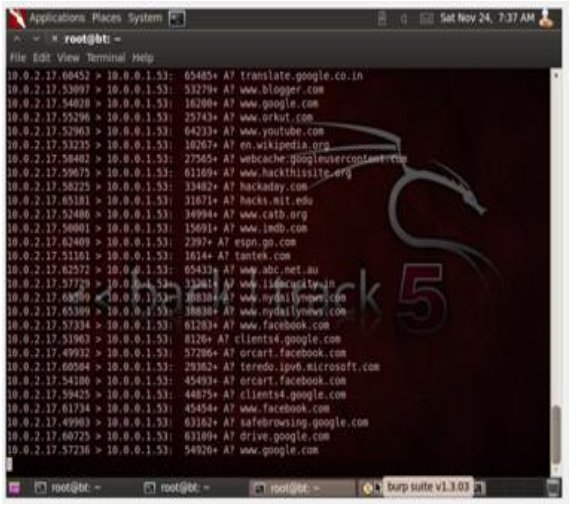
INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

deployed in the public places and these access points are kept unencrypted. When the access points are unencrypted maximum legitimate users will try to connect. When legitimate users connect to the fake access point, attack gathers the information. The various techniques are proposed to detect the fake access points. Among all the techniques some technique required extra hardware to detect the fake access points and some are the server-side techniques which are to costly. Client-side technique is the most common technique to detect fake access point .The main limitation of this technique is cumbersome processes and limited resources. In this paper, author proposed a novel approach to detect the fake access point. The proposed technique is based on the two approaches .One is received signal strength and other is online algorithm. We compare the signal strength of the access point with the legitimate access point, if the received signal strength is less than the threshold signal strength then access point is fake other wise not [5].

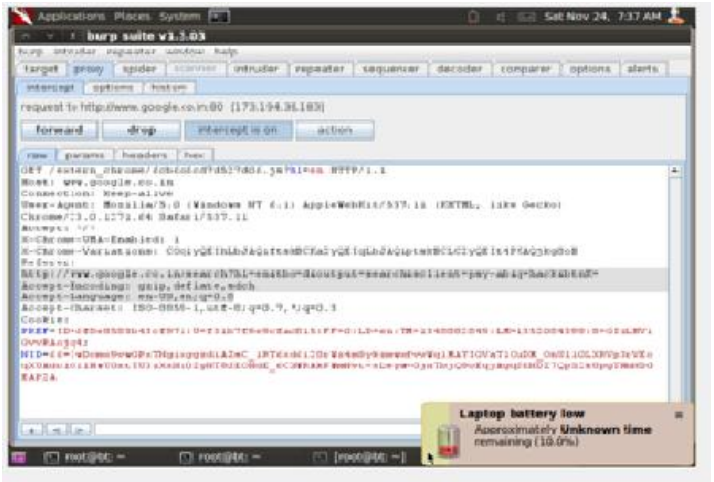
In this paper author proposed new technique to prevent session and cookie hijacking. The HTTP will be replaced by HTTPS for secure browsing. The author proposed technique will be implemented as an extension in Firefox .In this technique "one time cookies" are generated each time when client request to access the services of the server new cookie is generated and cookie integrity will be provided by HMAC [6].

3. Problem Formulation

The various types of security attacks are possible in infrastructure type of network. If we broadly classify these attacks as: active attack and passive attack .The most common type of active attack is session hijacking. The session hijacking attack is generally implemented with the honey pot. The fake access point acts like a honey pot. When user connects to a fake access point session hijacking possibility will be there. If fake access point is detected then we can prevent session hijacking .In our work, we will implement session hijacking with fake access point as shown in snapshot 1and 2. We use backtrack 5 to make fake access point and burp suit for session hijacking with fake access point.



Snapshot 1: DNS Spoofing to redirect network traffic



Snapshot 2: Session hijacking of Gmail

As, we have mentioned in the literature survey that server side detection of fake access is costly .In our work we mainly focus to develop new client side technique for fake access point detection for the prevention of session hijacking

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

4. Proposed Technique

Our new proposed technique is the hybrid type of technique .In the previous techniques we can detect the fake access point on the basis of received signal strength and beacon frames .In our technique the beacon frames generated by access point depends on the quality of the access point and beacon frames received by the legitimate user will also varies according to the climatic conditions. In our techniques we will fix a threshold number of beacon frames received by the receiver according to the climatic conditions and on the basis of access points quality .If the number of received beacon signals in fixed time slot will be less than the threshold value. The received number of beacon signals also varies according to the climate conditions and quality of access point .The threshold value also varies accordingly. We can declare that access point a fake access point.

5. Future Work and Conclusion

In this paper we conclude that session hijacking is active type attack 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 .In our work we also propose a client side technique to detect fake access point. In our future work, we will implement new proposed technique and compare results with the previous techniques.

References

[1] **"**Fast and accurate detection of fake points using non-crypto method in WLAN (2012)" International Journal of Communications and Engineering Volume 05– No.5, Issue: 03 March 2012.
[2] "A Mechanism for Detecting Session Hijacks in Wireless Networks (2010) **"**IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 9, NO. 4, APRIL 2010.
[3] Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad and Patrikck Traynor Converging Infrastructure Security (CISEC) Laboratory Georgia Tech Information Security Center (GTISC) Georgia Institute of Technology
[4] **"**A Comparative Study of Security Level of Hotmail, Gmail and Yahoo Mail by Using Session Hijacking Hacking Test (2008) "IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008.
[5] "Online Detection of Fake Access Points using Received Signal Strengths" Taebeom Kim, Haemin Park, Hyunchul Jung, and Heejo Lee Div. of Computer and Communication Engineering Korea University Seoul, Korea
[6] **"**One-Time Cookies: Preventing Session Hijacking Attacks with Disposable Credentials" Nick Nikiforakis1, Wannes Meert1, Yves Younan1, Martin Johns2, and Wouter Joosen11 IBBT-DistriNet Katholieke Universiteit Leuven, Celestijnenlaan 200A B3001, Leuven, Belgium.
[7] C. Siva Ram Murthy , B. S. Manoj,2007" Ad Hoc Wireless Networks, Architectures and Protocols"