Fake Access Point Detection and Prevention Techniques

Hemashu Kamboj, Gurpreet Singh

Department of information technology Lovely Professional University, Punjab

ABSTRACT----There are mainly two type of networks, wired and wireless. The wireless network is much vulnerable to security attacks as compared to wired network. In wireless networks there are both active and passive attacks are possible. The man-in-middle, session hijacking is the most common active attack today life. The session hijacking attack can be generally performed with the help of honey pot. The honey pot is just an access point without any security. 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, different techniques are purposed that helpful in detecting the fake access point. Most of the techniques are based on beacon frames for detection of fake access point. This paper shows how the fake access point takes place and work in real life and how the session is hijack. The fake access point creation and hijacking of session is done with the help of backtrack 5 and to detect and prevent different techniques are used.

KEYWORDS---- Fake Access Point, Beacon Frames, Cookies, Honey Pot, Session, Hijacking.

I. INTRODUCTION

The wireless networks can be broadly classified into two cetagories the 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 [5]. Infrastructure less networks, do not have fixed routers in which 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. In both network there are various types of active and passive attacks are possible. Passive attacks are those attacks in which attacks don't effect normal behavior of the network and simply sniff the network and in active attacks, attacker 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. Our work is to prevent session hijacking from fake access point to increase security. The session hijacking attack can be generally performed by using honey pots. The fake access point is the honey pot in our work which is an external device with the same standards as used in normal compuers and other devices. The legitimate user can connect to the unencrypted fake access point because don't know the difference between fake and orignal and when legitimate user accesses the services of the access point, attacker can hijack the session, cookies of the legitimate users. The legitimate user attract toward fake access point because don't have knowledge that who is fake and which one is original. A user who is already logged into 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 increasing because attackers are in great advantage of not having to waste hours and hours to crack a password or to try other different methods which needs more afforts and a lot of time, 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 or hack the session cookies etc. of 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. In the last section 4 future work and conclusion is presented.

II. Literature Review

A. Fast and accurate detection of fake points[1]

The users on the network are increasing drastically from last few years.In wireless networks the honey pots are used to perform session hijacking attack and we use external device which act as honeypot. The honey pots are used to monitoring and gathering

information ,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.

B. *A Comparative Study of Security Level of Hotmail, Gmail and Yahoo Mail[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.

C. *Online Detection of Fake Access Points using Received Signal Strengths[3]*

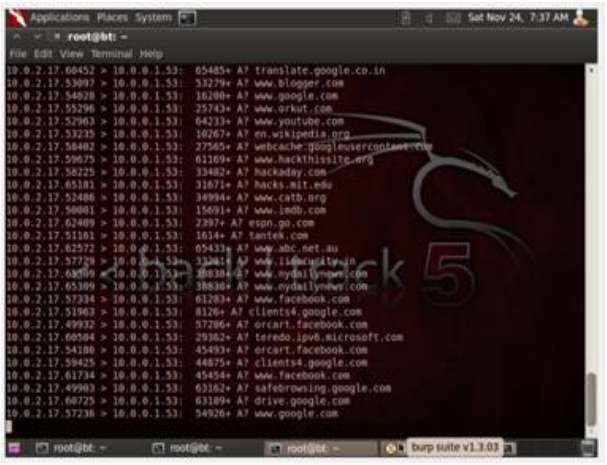
The wireless networks are gaining popularity day by day in todays life. The popularity of wireless local area networks (WLANs) increases the risk of wireless security attacks. The fake access points can be deployed in the public places and these access points are kept unencrypted. Fake access point is 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 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. In this paper, authoproposed 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 otherwise not.

D. *SessionShield: Lightweight Protection against Session Hijacking[4]*

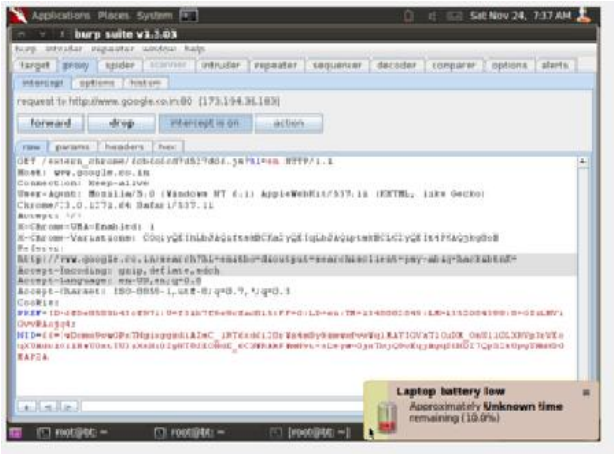
In this paper author proposed new technique to prevent session and cookie hijacking. The HTTP will be replaced by HTTPS for secure browsing. The author proposed technique will be implemented as an extension in Firefox .In this technique “one time cookies” are generated each time when client request to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

III. Problem Formulation

The session hijacking attack is generally implemented with the honey pot. The fake access point acts like a honey pot. So a fake access point is made using external network card with the help of backtrack 5 by following procedure according to backtrack 5. We use backtrack 5 to make fake access point and burp suit for session hijacking with fake access point.When user connects to a fake access point session hijacking possibility will be there. Snapshot 1 shows the DNS spoofing to redirect network traffic.



Snapshot 1: DNS Spoofing redirect the network traffic



Snapshot 2: Session hijacking of Gmail

Snapshot 2 shows that session is hijacks with the help ofburp suit tool inbuilt in backtrack 5. Cookies and session of user is hijack. This is the general procedure that shows after creating fake access point how to hijack session by using commands in backtrack. We discus various techniques in literature review that may help in detection of fake access point and we can prevent our session from hijacking.

IV. Conclusion and Future Work

In this paper we conclude after studying that session hijacking is active type attack and todays life has very bad impact on the network.The fake access points will work like honey pot and used to gather network information and for fake access point as a fake access point we use an external wireless network card which will be our honey. If a legitimate user connect to that fake access point then all the cookies passwords and important information is hijack by the attackers. If the fake access points are detected which will work like a honey pot then session hijacking will be prevented. In our future work, we will implement new proposed technique and compare results with the previous techniques.

ACKNOWLEDGMENT

I am very thankful to department of information technology (IT) of Lovely Professional University (LPU) Punjab India for providing the required facilities needed for the successful completion of this paper. I am also very thankful to those who have helped me directly or indirectly for accomplishment of this work.

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 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.

[3] "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

[4] Session Shield: Lightweight Protection against Session Hijacking Nick Nikiforakis1 , Wannes Meert1 , Yves Younan1 , Martin Johns2 , and WouterJoosen.

[5] C. Siva Ram Murthy , B. S. Manoj,2007" Ad Hoc Wireless Networks, Architectures and Protocols"