ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 7, July 2017

Preventive Solutions for Evil Twin Network Attack

[1] B. Lakshmi, [2]Sujatha Srinivasan
[1] Research Scholar Dept. of Information Technology School of Computing Sciences VELS University Chennai
[2]Head of the Dept Dept. of Information Technology School of Computing Sciences VELS University Chennai.

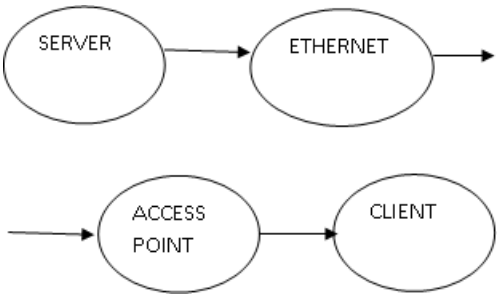
Abstract: ***An Evil twin is a Wi-Fi access point (AP) of attack. It is a version of the rogue (phishing) attack. It attacks the sensitive information such as usernames, passwords and credit card details from other Wi-Fi users with the same SSID (Service Set Identifier) name. An attacker interrupts the wireless users by gathering personal or corporate information without user knowledge. Existing studies detect Evil Twin attack in 802.11 wireless networks. Our proposed system is to detect Evil Twin attack in NAC (Network Access Control), because Network Access Control (NAC) technology provides solution for both authen¬tication of users and devices much like 802.11 as well as validation of the security of devices that are connected to a network. The main purpose proposed study is to provide a preventive solution for Evil Twin Attack. Wi-Fi mask tool which is the extension of wire shark tool is used for prevention.***

Keywords- ***SSID, Evil Twin, Wire shark, Wi-Fi mas.***

I. INTRODUCTION

We are trying to develop an algorithm which will be embedded into all OS code which will have the capacity to detect Wi-Fi network with the same service set identifier popularly called SSID. SSID is an unique identifier sent with packets over Wi-Fi networks. An evil twin attack creates the fake SSID which belongs to the Wi-Fi users. The user will access the fake SSID and enter the password. The attacker eavesdrop the password and access the information. Therefore this attack is hard to find. In this study we propose an algorithm to avoid connecting to the unknown network with the same SSID. The rest of the paper is organized as follows: Section II gives an overview of the two Access Control technologies widely used in the literature. Section III compares and contrasts the two techniques bringing out the similarities and differences. Section IV reviews the literature on studies that have proposed and developed solutions for tackling evil twin attacks. Also a discussion that brings out the limitations of existing systems is given. Section V gives a brief discussion about the existing Wireshark tool and proposes a wi-fi mask tool as an extension of wireshark tool to overcome the evil twin attack. The working methodology of the proposed model is explained. Section VI concludes with summary and future research directions.

Normal AP



Evil twin AP

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 6, June 2017

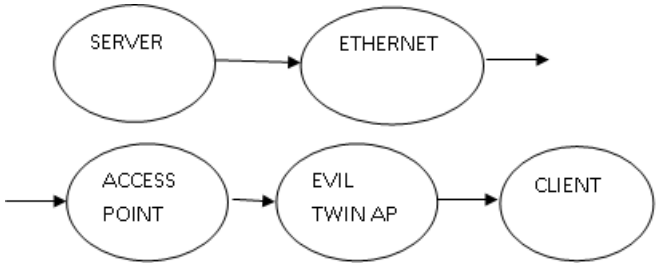


Fig 1 Normal and Evil twin Access Points

II. OVERVIEW OF 802.11AND NETWORK ACCESS CONTROL

A. MAC – 802.11

802.11 are a medium access control (MAC) used for implementing wireless local area network (WLAN) computer communication developed by IEEE. 802.11 technology developed by the U.S. Federal Communications Commission in 1985 that released the ISM band for unlicensed use. In 1991 NCR Corporation/AT&T (now Nokia Labs and LSI Corporation) developed 802.11 in Nieuwegein, the Netherlands. They use the technology for cashier systems. The first wireless products were brought to the market under the name WaveLAN with raw data rates of 1 Mbit/s and 2 Mbit/s.

Vic Hayes developed IEEE 802.11 for 10 years, and called as the "father of Wi-Fi" designed the initial 802.11b and 802.11a standards within the IEEE.

In 1999, the Wi-Fi Alliance was formed as a trade association to hold the Wi-Fi trademark under which most products are sold.

B. Network Access Control (NAC)

Network Access Control (NAC) is an approach to computer security used for endpoint security technology (such as antivirus, host intrusion prevention)and also used for user or system authentication and network security. Cisco first introduced NAC in late 2003/early 2004, it was network admission control. Gartner was one of the first groups to start using NAC as a generic term which is referred as pre-connect network access control. NAC types of functions are developed released in April of 2004. The endpoint policy compliance and enforcement tool was released in 2003. Microsoft announced their NAP initiative for Longhorn in later 2004/early 2005. In the mid of 2005 there were many companies using NAC. By RSA 2006 NAC was taking the security world by storm.

NAC restricts the data that each particular user can access, as well as implementing anti-threat applications such as firewalls, antivirus software and spyware-detection programs. Fig 1 represents the normal and evil twin APs.

III. SIMILARITIES AND DIFFERENCES OF NAC AND 802.11

A. Similarities

- 802.11 and NAC both had standard strong authentication mechanisms and directory systems.
- All ports are set to unauthorized (or similar state) until successful authentication is completed
- Dynamic assignment of VLANs is typically used to control access levels for different types of users

B.Differences

- NAC provides compliance validation of endpoints is used in determining access policy.
- NAC is not dependent on supplicant
- NAC can provide post-connect monitoring and controls i.e., some solutions can monitor endpoints and network connections and some solutions can react to security systems such as an IDS/IPS.

IV. REVIEW OF LITERATURE

Payal Bhatia, Christine Laurendeau and Micheal Barbeau [2] detect evil twin attack by placing 4-square antenna transmitter on each receiver. This method detects 100% attack only when the transmitters are present in non-identical zones but detect 53% attack only when the transmitters are present in identical zones[2]. **Yimin Song, Chao Yang and Guofei Gu** used TMM (Trained Mean Matching) and HDT(Hop Differentiating Technique).TMM is a training based algorithm which is time consuming and not in practical use so they go to HDT which is a non-training based algorithm to detect attacks. The HDT is not suitable for network saturation[3]. **Harold Gonzales, Kevin Bauer, Janne Lindqvist, Damon McCoy, Douglas Sicker** used Context-leashing and (Secure Shell) SSH-Style authentication protocol.SSH provide a secure channel over an unsecured network. It generates pair of public-private key to encrypt the connection. Context-leashing does not provide authentication, integrity or privacy to prevent attack.[1] **Saranya and V.Pugazhenthi** used UnMASK (Utlizing Neighbor Monitoring for Attack Mitigation) method that detects the malicious node but malicious nodes form collision with unmalicious nodes21 **Prabhash Dhyani** provides solutions for Honeypot attack. The solutions are user should not accept untrusted file. Clients should turn off wi-fi if it is not in use[6]. **Sachin R.Sonawane, Sandeep Vanjale, Dr.P.B Mane** used Fake Broadcast packets scheme to detect evil twin attack. It is suitable for both wired and wireless networks. But the drawback is it is not supported in network partitioning[7]. **Chao Yang, Yimin Song and Guofei Gu, Member of IEEE** used Evil Twin Sniffer approach. They used the techniques of both existing system TMM and HDT to implement ETSniffer. ETSniffer is suitable for 802.11open source. But the drawback is it can't identify the middle attack in the WLAN[8]. **Fabian Lanze, Andriy Panchenko, Thomas Engel and Ignacio Ponce** used Differentiated attacker model. It is not suitable for all software tools and need large scale evaluation. It uses the aircracking suite software tool to detect the fake Access Point[9]. **Maheshkumar Ramrao Gangasagare** used RTT- Round Trip Time approach. It provide the information about authorized APs, rouge APs and wired nodes. This technique identify neighbor AP as rogue AP. It differentiate the wired network users and wireless network users. **Sachin R. Sonawane ,Sandeep P.Chawan and Ajeet A. Ghodeswar** used RAP Detection (Rogue Access Point) method. It is based on learning free algorithm and learning based algorithm. It used TMM and HDT algorithm to detect the attack but it not able to identify the rogue APs[10].

TABLE I SUMMARY OF SYSTEMS FOR HANDLING EVIL TWIN ATTACKS

Ref	Methodology	Limitations/ Research Gaps
[2]	HPB- Hyberbolic Position Bounding	It detects 53% of attacks only when the transmitters are available in particular zones
[3]	TMM - Train Mean Matching	It is not implemented practically and its time consuming
[3]	HDT- Hop Differentiating techniques	It is not supported for spontaneous network movement changes
[1]	Context-Leashing and SSH-Style authentication protocol	It is not suitable for multiple Access points
[4]	Jamming Techniques	it will work under 100 m ranges
[6]	Resolving remedies for Honeypot attack	Clients should turn off wifi if it is not in use.
[5]	UnMASK (Utlizing Neighbor Monitoring for	Malicious nodes form collision with unmalicious

	Attack Mitigation)	nodes
[7]	Fake Broadcast packets scheme	Not supported in network partitioning
[8]	ETSniffer(Evil Twin Sniffer)	Can't identify the middle attack in the WLAN
[9]	Differentiated attacker model	Does not suitable for all software tools and need large scale evaluation
	RTT- Round Trip Time	To make sense of knowledge of an authorization roll of AP's
[10]	RAP Detection (Rogue Access Point)	Not able to identify rogue AP's

Discussion

The literature review gives a few highlights into the limitations in existing systems for evil twin attack. Table I gives a summary of the different techniques proposed to handle evil twin attacks. There are some research gaps in existing algorithms. HPB- Hyberbolic Position Bounding algorithm detects only 53% of attacks when the transmitters are available in particular zones. TMM - Train Mean Matching algorithm is not implemented practically and its time consuming. HDT- Hop Differentiating techniques are not supported for spontaneous network movement changes. Context-Leashing and SSH-Style authentication protocol is not suitable for multiple Access points. Jaming Techniques will work under 100 m ranges. For Honeypot attack Clients should turn off wifi if it is not in use. In UnMASK (Utlizing Neighbor Monitoring for Attack Mitigation)method malicious nodes form collision with unmalicious nodes. Fake Broadcast packets scheme algorithm was not supported in network partitioning. ETSniffer(Evil Twin Sniffer)algorithm can't identify the middle attack in the WLAN. Differentiated attacker model does not suitable for all software tools and need large scale evaluation. RTT- Round Trip Time does not have knowledge of an authorization roll of AP's. RAP Detection (Rogue Access Point) not able to identify rogue AP's. Protection Mechanism transfer cryptographic key for authentication protocols. These gaps are identified and a solution to overcome the above limitations is provided by the system proposed in the following section.

V. THE PROPOSED WI-FI MASK TOOL FOR EVIL TWIN ATTACK DETECTION

A.Wireshark tool

Wireshark tool is a network packet analyzer. It captures the network packets and displays the entire details of packet data. It is a measuring device and it examines what is going inside the network cable.

It is suitable for

- Troubleshoot network problems
- Security problems
- Debug protocol implementations

Drawbacks:

- Wireshark is not an intrusion detection system. It will not give warning when an unauthorized person enters into the network.
- Wireshark will not manipulate it only measure what is happening inside the network.

To avoid these bugs we are going to modify this tool as **wi-fi mask tool** it will work above 100 m range by using NAC.

Methodology

The proposed wi-fi mask tool works as follows:

I. Available for UNIX and Windows, Capture live packet data from a network interface. ˆ
II. Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs. ˆ
III. Display packets with very detailed protocol information and Save packet data captured.ˆ
IV. Export some or all packets in a number of capture file formats. Filter packets on many criteria. ˆ
V. Search for packets on many criteria.Colorize packet display based on filters. Create various statistics. ˆ
VI. It allows the user to put network interface controllers that support promiscuous mode into that mode, in order to see all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic.

VI. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

In this paper we have reviewed literature on evil twin attack detection. Some of the methodologies protects the user from the evil twin attack but not beyond 100 m ranges. Some used client side tool-wireshark for capturing packets on wireless networks. It will manually analyze packets in and out as well as rouge APs. But it is very expensive and does not capture the attack on local systems. To avoid these bugs an algorithm which is a client side tool named **wi-fi mask** tool which is an extension of **wireshark** tool is proposed**.** Wifihop is a client side tool for evil twin attack. But Wifihop tool identifies a normal AP as rogue AP and works only under 100m range. But the proposed tool will work above 100 m range by using NAC. To avoid cost consumption we have proposed to use AWS S3 (Cloud Computing) to establish connections in large networks. We are implementing the system using NS 2 simulator. As future work we propose to test the system on other networks and also to implement the system for different devices and ranges.

References

[1] H. Gonzales, K. Bauer, J. Lindqvist, D. McCoy, and D. Sicker, "Practical defenses for evil twin attacks in 802.11," *GLOBECOM - IEEE Glob. Telecommun. Conf.*, 2010.
[2] P. Bhatia, "Detecting and Localizing Transmitters in a Wireless Evil-Twin Attack Background of HPB."
[3] Y. Song, C. Yang, and G. Gu, "Who is peeping at your passwords at starbucks? - To catch an evil twin access point," *Proc. Int. Conf. Dependable Syst. Networks*, pp. 323–332, 2010.
[4] A. Cassola, W. Robertson, E. Kirda, and G. Noubir, "A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication," *Netw. Distrib. Syst. Secur. Symp.*, pp. 1–15, 2013.
[5] J. Saranya and V. Pugazhenthi, "Mitigating Spoofing Attacks through Received," pp. 70–74, 2014.
[6] P. Dhyani, "New Avatars of Honeypot Attacks on WiFi Networks," no. 3. .
[7] S. R. Sonawane and S. Vanjale, "Wireless LAN Intrusion Prevention System (WLIPS) for Evil Twin Access Points," vol. 8491, pp. 2–5, 2013.
[8] C. Yang, Y. M. Song, and G. F. Gu, "Active User-Side Evil Twin Access Point Detection Using Statistical Techniques," *Ieee Trans. Inf. Forensics Secur.*, vol. 7, no. 5, pp. 1638–1651, 2012.
[9] F. Lanze, A. Panchenko, I. Ponce-Alcaide, and T. Engel, "Undesired Relatives: Protection Mechanisms Against The Evil Twin Attack in IEEE 802.11," *Proc. 10th ACM Symp. QoS Secur. Wirel. Mob. networks*, 2014.
[10] C. Science and S. Engineering, "Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN," vol. 3, no. 10, pp. 1232–1237, 2013.