ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Detection & Analysis of Evil Twin Attack in Wireless Network

Vishwa Modi
M.Tech Cyber Security
Raksha Shakti University,
Ahmedabad, India

Chandresh Parekh
Department of Telecommunication
Raksha Shakti University
Ahmedabad, India

Abstract: Due to increasing demand of wireless internet access open Wi-Fi internet service is available at public places and secured Wi-Fi internet service is available at private/commercial places. Device can connect to any wireless access point by identifying only two identifier - the network name and MAC address of access point. The widespread use of wireless network gives rise of various security threat among which is Evil Twin Attack. The presence of such security threat in network causes significant loss of information. In this paper, we discussed Evil twin Attack and its effect in wireless network. We also discussed various solutions proposed by researcher. We present a very simple solution by considering certain ways of evil twin attack to detect Evil Twin Access Point to prevent attack. We have used RTT and number hops between client and server based technique and de-authentication detection between client and legitimate access point based technique.

Keywords: Access Point, BSSID, De-authentication frames, Evil Twin Attack, External IP address, SSID, Rogue Access Point, Wi-Fi network

I. INTRODAUCTION

Due to advancement in wireless technology demand of wireless network services are increased at every places. Because of that wireless communication infrastructure services and mobility of the world have been proliferating with the goal of meeting rapidly increasing demands. Earlier the people were used wire or cable to connect to the internet. Today wireless technology gives more facility, intendancy and mobility over wired network [1].

At public places such as fast food restaurants, café, shopping malls public Wi-Fi service is provided. So that users are able to access wireless internet service at these places without paying any money. For ease of access this public Wi-Fi services are not providing any kind of security to the user. This public Wi-Fi is the most attractive target of attacker for intercepting, collecting data such as user's user name, password and other information. As such security threats and vulnerabilities associated with the protocol layers are typically protected independently at each one layer to meet the security requirements of wireless network such as authenticity, confidentiality, integrity and availability. But still attackers are targeting the Wi-Fi networks in different ways to intercept the network traffic [1][2].

Evil Twin Attack

Evil Twin attack is performed by creating rogue access point by spoofing SSID, BSSID, Channel, IP address, etc. of legitimate access point. Generally every access point broadcasts beacon frames to notify existence of it to all the wireless devices. This beacon frame contains SSID, BSSID, Timestamp, channel and many more fields. The users can connect to these access point. Because of that the client can able to see access point and connect to that access points. So that attacker capture this beacon frame to make rogue access point using same SSID and BSSID of legitimate access point. When access point has higher signal strength then wireless devices are automatically get connect with it. So that to take advantage of this feature, the attacker may also increase the signal strength of rogue access point. As a result wireless devices unknowingly automatically get connected with this access point [1][6].

When a client connects access internet services through this malicious access point, the attacker can sniff the network traffic such as username, password, unencrypted credential and other critical data by monitoring and intercepting the network traffic generated through wireless client's device. It's becoming very challenging job to detect the Evil Twin Attack. There are many ways to launch Evil Twin Attack. Different types of tools are available for performing evil twin attack [9]. So that attackers can easily create attack using such tools.

Subsequent figure shows two scenarios of performing evil twin attack for which we have proposed detection method.

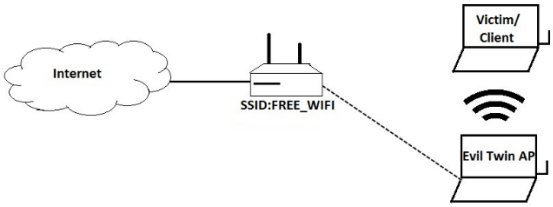

Figure 1. Evil Twin AP with same SSID, BSSID and uses LAP for internet service

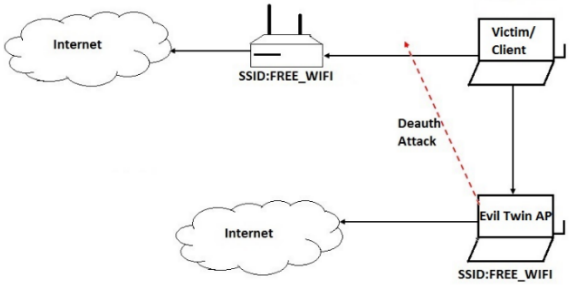

Figure 2. Evil Twin AP with same SSID, different BSSID and Deauth client from LAP

In Figure 1 the attacker spoofs SSID and BSSID of legitimate access point (LAP) and uses them to create evil twin access

point. Here evil twin access point provides internet service to the client by connecting his access point with the legitimate access point. So that evil twin AP working as man in the middle by forwarding network traffic between client and legitimate access point. Therefore attacker is able to capture all the traffic of client who is connected to him [7].In Figure 2 attacker spoofs only SSID of legitimate access point and uses it to create evil twin AP. In this case attacker may use different internet service provider than the legitimate access point having. An attacker sends de-authentication frame using MAC address (BSSID) of legitimate access point to all the clients to disconnect them from legitimate access point. So that they can only able to connect with the evil twin AP [1][8].

II. EFFECT OF EVIL TWIN ATTACK

1. Evil twin access point forwarding packets from client to legitimate access point in man in the middle position. In this case attacker can eavesdrop and modify network traffic of the victim [4].
a) Steal credentials from services such as email, social media, paypal, etc. This could be accomplished with tools such as SSL Stripper. The attacker could use these credentials to access his victim's accounts.

The attacker can steal or alter information, use services, send messages on behalf of his victim, transfer money. The attacker might even sell these account credentials.

b) Collect personal information. This could be used to identify users

c) Access a client using vulnerabilities in the client's OS.
2. In private and enterprise network, stealing of network credentials is possible because public networks do not use network credentials [3].

To authenticate the user to the Access Point these credentials, often a combination of username and password, are used. An attacker can impersonate his victim and gain access to the network by using the stolen credentials. This access can be mistreated to anonymously access the Internet and hide behind his victim identity.

The attacker can also use his victim's credentials to intentionally frame his victim. This would require the network to track the traffic of his users, in order to establish a link between the incriminating evidence and the victim.
In some cases network credentials are re-used for different purposes.

3. An attacker can only identify the user if the network distinguishes between users. This is only conceivable with enterprise networks as these networks use a combination of username and password as network credentials. These usernames are needed to identify the user.

If the attacker is able to identify the user he can combine this information with the time and place in order to track the user's movement (this can be enhanced with multiple rogue APs) [5].

4. Estimating previous movements.

An attacker could eavesdrop on probes request sent by the victim's device. These probes request expose the names of previously connected networks. The attacker can query online databases containing names and locations of wireless networks, in order to find the locations possibly visited by his victim. He could also inspect the names to determine if it might be a work or home location.

III. METHODOLGY

A. Attack creation

In order to implement our detection technique we created rogue access point to perform Evil Twin Attack. In which attacker disconnects clients from the legitimate access point by launching de-authentication attack and in another way evil twin access point is behaving as man in the middle by forwarding traffic between client and legitimate access point and evil twin access point uses different ISP network to provide internet service to users .

B. Test bed

In order to assess our proposed method we created rogue access point using external wireless adapter having chipset Atheros USB 2.0 WLAN in kali linux using Airmon-ng, airbase-ng, airodump-ng aireplay-ng. Another system which is used as a client machine. Client system has kali linux operating system which is used for detection purpose.

C. Procedure

Client first connect with access point AP1 and gather RTT, number hops between client and any arbitrary server like www.google.com and External IP address of AP1. Then connect with another access point having same SSID (Name of Access Point) as of the previous one. Our algorithm will compare SSIDs and BSSIDs of both access point. If SSID and BSSID of both access points are same then get the External IP address (IP address of ISP) of access point to whom connected and compare it with the previously connected access point. If External IP address of both access points are same then get RTT between client and server. If RTT value for current access point is greater than the previous access point then display alert like connection is not secure. Then for confirmation of Evil Twin Attack which is behaving as man in the middle get number hops between client and server. If number of hops for current access point is greater than the previous one then current access point (AP2) to whom connected is Evil Twin access point. On the other hand if RTT and number hops for previously connected access point AP1 is greater than the currently connected access point AP2 then AP1 is Evil Twin access point.
In second case if SSID and BSSID of both access points are same and External IP is different because rogue access point uses different ISP than the legitimate access point then alert client about possibility of Evil Twin Access Point.
In third case if SSID of both access points are same and BSSID of them are not same then check for deauth attack on legitimate access point which disconnect the client from legitimate access point and also prevent to reconnect it. Detect this deauth frames for legitimate access point's MAC address and alert about it.

IV. RESULT & DISCUSSION

First we have created evil twin access point by spoofing the identifiers of legitimate access point on one machine and

detection of attack on another machine. We can able to see in our Fig. 3 two Wi-Fi access point having same name (like FREE_WIFI) on other (client) machine.

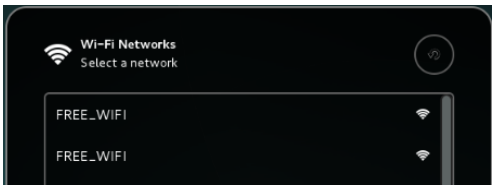

Figure 3. Two Wi-Fi networks with same name

Connected with any one of access point called AP1 and stored information (External IP, RTT, number of hops) as shown in Figure 4.

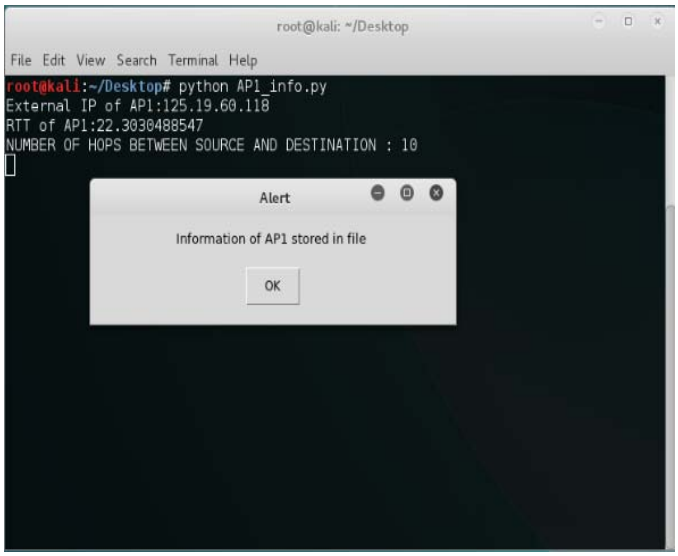

Figure 4. Captured & stored information for AP1

Then switched to another access point called AP2. Compared SSID and BSSID of both access points. Then external (ISP) IP address for both are compared. These identifiers were same then compared the RTT and number of hops of recently connected access point AP2 with previously connected access point AP1. For AP1 both the values are greater than the AP2. So alert was generated about evil twin.

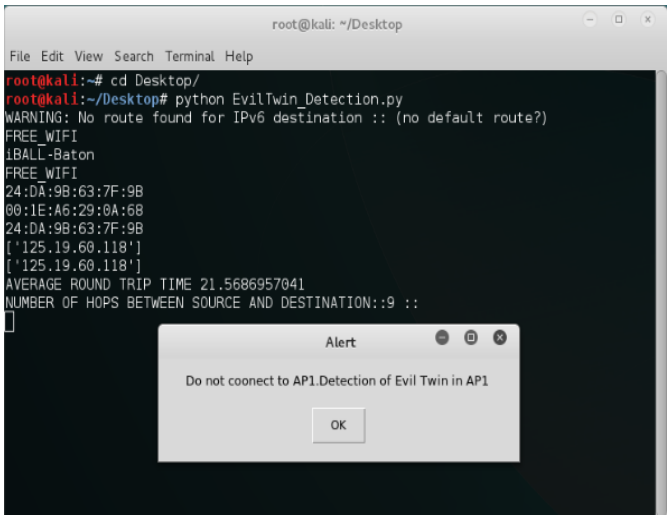

Figure 5. Previously connected access point (AP1) is Evil Twin

Both the access point have different External (ISP) IP addresses. So warning of possibility of Evil twin attack displayed as below Figure 6.

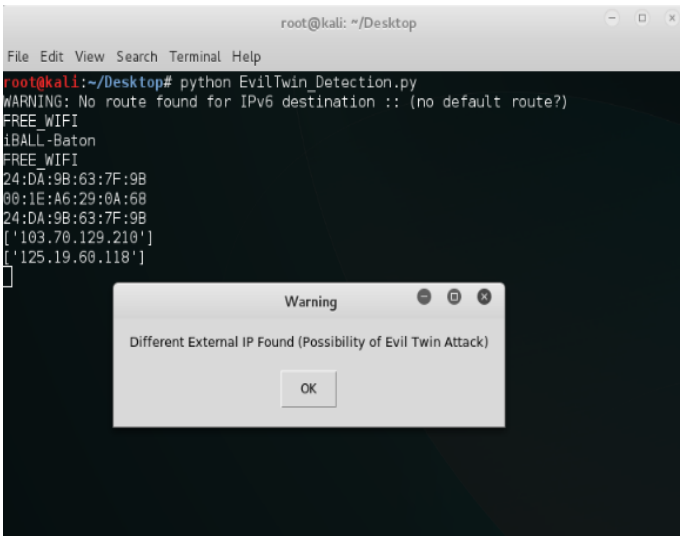

Figure 6. Different External IP of Same access point

Second case both access points had different BSSID then checked that any one of them was performing deauth attack on another one.

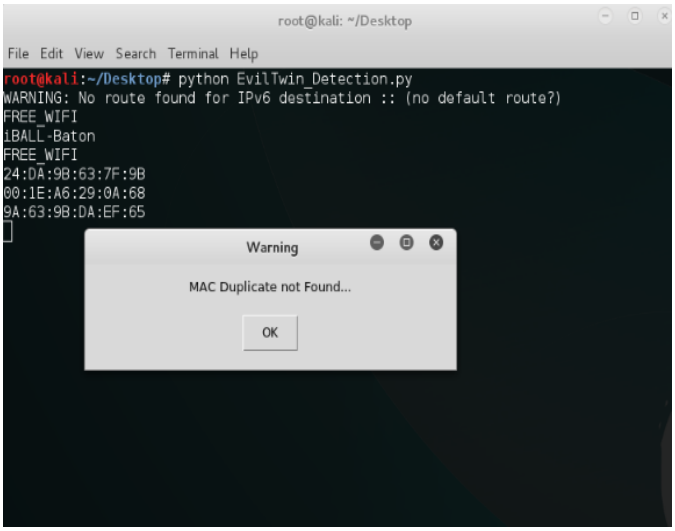

Figure 7. Different MAC Found

Continuos deauth frame detected from one's MAC address so it might be under the attack of Evil Twin Access Point (in Figure 7 & Figure 8).

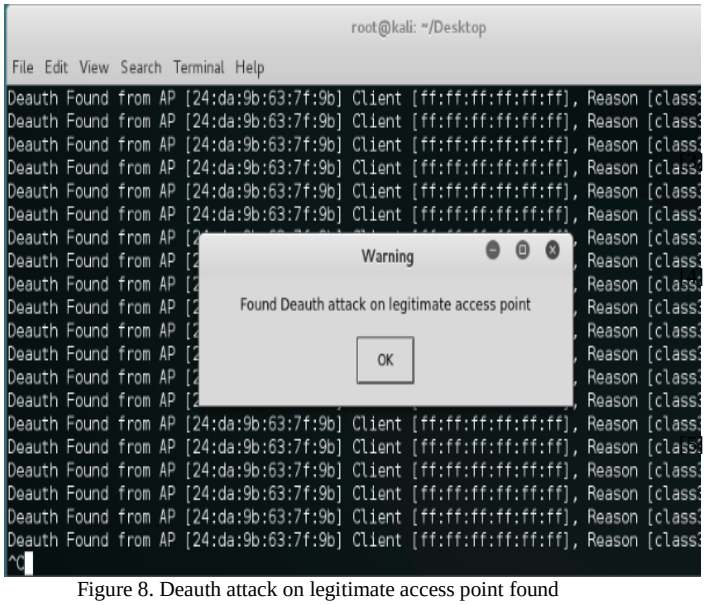

Figure 8. Deauth attack on legitimate access point found

V. CONCLUSION & FUTURE WORK

Wireless network is prone different type of attack. Here we considered and discussed about Evil Twin attack. The proposed technique contributes to detection of Evil Twin Attack. We considered particular scenarios of evil twin attack and proposed solution for them.

Our detection technique can be further enhanced by introducing more variables and considering different possibility of evil twin attack.

VI. REFERENCES

[1] Vishwa Modi, Asst. Prof. Chandresh Parekh, "Detection of Rogue Access Point to Prevent Evil Twin Attack in Wireless Network", International Journal of Engineering Research & Technology (IJERT), Vol. 6 Issue 04, April-2017, Pg. 23-26.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Yulong Zou, Senior Member IEEE, Jia Zhu, Xianbin Wang, Senior Member IEEE, and Lajos Hanzo, Fellow IEEE, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination, Pg. 1727-1765.

Omar Nakhila, Afraa Attiah, Yier Jinz, and Cli_ Zoux. Parallel active dictionary attack on WPA2-PSK Wi-Fi networks. In Military Com- munications Conference, MILCOM 2015-2015 IEEE, pages 665-670. IEEE, 2015.

Anil Kumar, Partha Paul, "Security Analysis and Implementation of a Simple Method for Prevention and Detection against Evil Twin Attack in IEEE 802.11 Wireless LAN", 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), Pg. 176-181.

Nazrul M. Ahmad, Anang Hudaya Muhamad Amin, Subarmaniam Kannan, Mohd Faizal Abdollah, Robiah Yusof, "A RSSI-based Rogue Access Point Detection Framework for Wi-Fi Hotspots", 2014 IEEE 2nd International Symposium on Telecommunication Technologies (ISTT), Langkawi, Malaysia (24-26 Nov 2014), Pg.104-109.

[6] Volker Roth, Wolfgang Polak and Eleanor Rieffel, "Simple and Effective Defense Against Evil Twin Access Points", 2008 ACM conference on Wireless network security, Pg. 220-235.

[7] Omar Nakhila, Cliff Zou, "User-Side Wi-Fi Evil Twin Attack Detection Using Random Wireless Channel Monitoring", IEEE Milcom 2016 Track 3 - Cyber Security and Trusted Computing, Pg. 1243-1248

[8] Hao Han, Bo Sheng, Member, IEEE, Chiu C. Tan,Member, IEEE,Qun Li,Member, IEEE, and Sanglu Lu,Member, IEEE "A Timing-Based Scheme for Rogue AP Detection" IEEE Transactions On Parallel And Distributed System (2011), Pg. 1912-1925.

[9] Fabian Lanze, Andriy Panchenko, Ignacio Ponce-Alcaidey, Thomas Engel, Hacker's Toolbox: Detecting Software-Based 802.11 Evil Twin Access Points, 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Pg 225-232.