IJCSI International Journal of Computer Science Issues, Volume 14, Issue 1, January 2017
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org https://doi.org/10.20943/01201701.6068

Mitigating Evil Twin Attacks in Wireless 802.11 Networks at Jordan

Sinan Ameen Noman[1], Malik Qasaimeh[2], Raad Al-Qassas[3], Haitham Ameen Noman[4]

**[1] Department of Computer Science, Princess Sumaya University for Technology
Amman, 11941, Jordan**

**[2] Department of Computer Science, Princess Sumaya University for Technology
Amman, 11941, Jordan**

**[3] Department of Computer Science, Princess Sumaya University for Technology
Amman, 11941, Jordan**

**[4] Department of Computer Science,
Kuala Lumpur, 54100, Malaysia**

Abstract

Thinking twice before connecting to a public Wi-Fi at a coffee shop, hotel or an airport lounge is a must nowadays. Every Wi-Fi user should be cautious whether this free Wi-Fi hotspot that is allowed to be connected to is authentic or nothing but a rogue access point. Rogue access points (aka evil twin access point) allows the attacker to eavesdrop network traffic and to intercept the victims exchanged data or to even to alter the data while en route. The objective of this study that is going to be conducted somewhere in Jordan is to assess the security level in this area and to put a remedy to the weaknesses wherever found. This paper gives a statistical survey to illustrate the threatening level of such fake access point then to analyze the weaknesses and strengths of security measures in order to raise people awareness toward this kind of attacks.

Keywords: Wi-Fi, Evil Twin Attack, Rogue Access Point, Eavesdrop

1. Introduction

The 802.11 has been launched in 1997 by IEEE, which is part of 802 standards [1]. That means the architecture of the Wi-Fi is akin to the other networks of the 802 family especially the Ethernet network standard 802.3. This standard has led too many people to call the 802.11 standard as "Wireless Ethernet". The wireless network uses radio waves, just like cellular devices, walkie-talkie and TVs. These devices can send and receive radio waves on different frequency. The Wireless network (802.11) transmit at frequencies 2.4Ghz or 5Ghz.The 802.11 frequency are higher than the frequencies that used for walkie-talkies, cellular device and TVs [2]. The device that has a higher frequency will have the ability to carry more data. The 2.4Ghz divided the network into 11 channels and in practice only 3 channels can be used together (1,6 and 11) . All wireless networks have a unique name, known as SSID, which is stand for service set identifier. The SSID can discriminate between the other SSID names and makes it easily for the users to find and connect to the desired network. After connecting to the desired network, the user should correlate with the access point after completing the optional authentication. The network authentication can be either Open or Shared Key. The open network authentication allows anyone to access the network while the shared network key requires a key that is shared to all people across the network. A WarBiking Riding Project [3] involves around London streets looking for a wireless connection by using computer-equipped mountain bike to sneak a peek at the people who are using these public Wi-Fi networks, and unfortunately, people in London are all happy to connect to the unsecured wireless network without using any type of protection. The survey has been made on 81,743 networks in London, 29.5% were using Wired Equivalent Privacy (WEP) algorithm or no security at all, 52% of networks were using Wi-Fi Protected Access (WPA) algorithm, and only 17% of networks are using WPA2 encryption. The man behind WarBiking project created an open wireless network point in a busy part of London and name it "DO NOT CONNECT "and the result shown is somewhat alarming, if not downright disgraceful. 2% of more than of 812 victims were using VPN Services, 12% were using HTTPS, 8% were using insecure email, and

78% were using HTTP. According to XIRRUS Wi-Fi Network, A study in UK has been conducted by XIRRUS Wi-Fi Network [4], there are 8.5 million Wi-Fi hotspots available in UK. XIRRUS has surveyed over 300 respondents between 18 and 75 about how they connect to the internet, what do they do when they are connected, and how they connect .79% of respondents said that they did not trust security measures on public Wi-Fi, while 62% of respondents said they still connect to public networks. The study also showed that 58% of the survey respondents admitted to use public Wi-Fi but only 7% had actually installed VPN service on their devices to protect their confidential data. According to a poll that has been conducted by Kaspersky Lab in 2012 [5], 32% of more than 1600 respondents said that they are using public Wi-Fi networks regardless of whether the public networks have an encryption method to protect their costumers from eavesdropping. Internet usage has been increased evidently; many people nowadays are used to be connected to the internet most of the time by using their own notebooks, desktops, smartphones or tablets. People usually prefer to use Wi-Fi rather than any other medium. The reason of this desire is because Wi-Fi consumes less power compared with other medium like 3G and 4G and also because of its affordable cost. According to a Survey that has been conducted in Jordan using Google Survey, there are about 73% of 100 surveyed people in Jordan not protecting themselves when they are connected to a public Wi-Fi network. This survey indicates the high likelihood of trust shown by people toward public Wi-Fi networks. This result shows the significant role of awareness and perception that must be raised among the people. However, there should be a seamless solution that can help people to be protected from this kind of attacks besides raising their awareness. The public needs to know how they should deal with public Wi-Fi network and how risky is it when they connect to public unsecured access point. Moreover, they need to know how easy it can be for the hackers to create a Wi-Fi rogue access point to intercept the sensitive credentials and credit cards of all hosts that are connected to their fake access point. Technically, every person is vulnerable to evil twin attack even if the person was communicating with an access point that requires a security password such as (WEP, WPA, WPA2). For Example, once the victim connects to a particular network, the victim opts to save the network as preferred one in the operating system itself so that when a victim starts looking for a network, a probe messages will be automatically sent from the operating system looking for that specific network. Accordingly, the attacker will intercept the probe messages by using some Linux tools and will create a new network with the same SSID name of the attacked network. The victim operating system will be lured to automatically connect to the associate access point the attacker just created. At the same time the attacker might send a continuous de-authentication broadcast attack to disable any ranged network to force the user to connect to solely the rogue network. In this paper, we are interested in number of people who prefer to use internet in a public place, number of people who prefer to use Wi-Fi in public places, investigating what people do when they are using Wi-Fi in public places, critical of the application used by users in public places, and see if the education level impacts on the way of using the internet.

Our contributions are as follows:

- Attacker scenarios using Evil Twin Attack and its relevant mechanism.
- Conducted a statistical survey in Jordan to illustrate the threatening level of rogue access point.
- Proposed a set of recommendations that can minimize the threats of Evil Twin Attack.

The remainder of this paper is organized as follows. Section 2 describes Evil Twin Mechanism and how easy this attack can present danger on users in public places. Section 3 presents Evil Twin attack scenarios. Section 4 introduces the survey methodology and presenting survey results. Section 5 introduces the recommendation concerning how the users should protect themselves from Evil Twin Attack. Section 6 describes the related work. Finally; Section 7 presents our conclusions.

2. Evil Twin Mechanism

Fake access points are generally easy to set up, the attacker needs to be equipped with a laptop with Linux operating system, a wireless adapter that supports injection like Alfa wireless adapter. The attacker should switch the Alfa wireless card into a monitor mode by using “airmon-ng” tool, to obtain the ability to discover all network and get all valuable information of the ranged networks such as “BSSID, Power, Beacons, Channel, and ESSID “it simply can be done by using airodump-ng tool as it shown in figure 1.

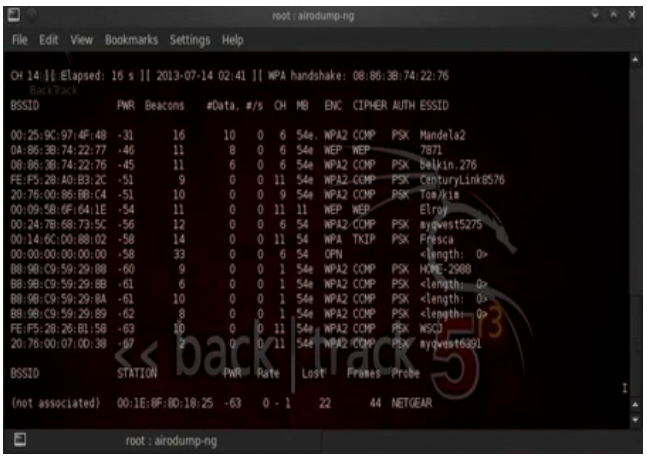

Fig. 1 Discovering network information by using airodump-ng tool.

The attacker is now ready to create an access point with the same SSID to deceive the victim by using "airbase-ng" tool. The only thing that the attacker should do is to force the victim to disconnect from the access point and connecting to the attacker's rogue access point and this can be done by using "aireplay-ng" tool. The "aireplay-ng" tool is used to de-authenticate the victim and strong strength to force the victim to connect to the rogue access point as it shown in the figure 2.

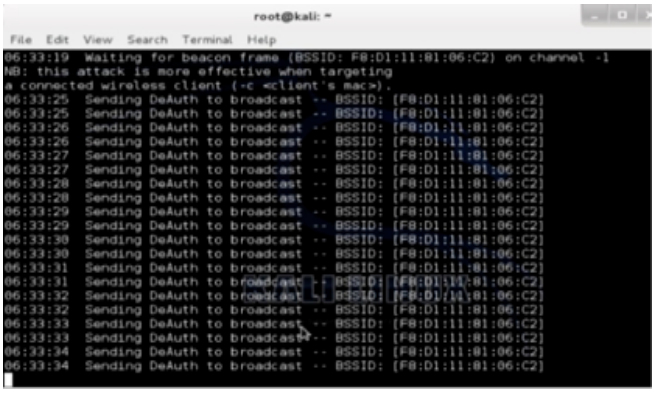

Fig. 2 De-Authentication attack using aireplay-ng tool

De-authentication attacks can be detected easily nevertheless, there is no concurrent solution to prevent de-authentication attacks. However, the new standard 802.11 ac promises to provide protection only to the networks that implement encryption, yet it still does not provide protection to unencrypted networks. After that, the attacker will create a rogue access point with the same SSID to deceive the victim. The rogue access point will have a high-power signal strength. The victim will try to re connect to the network, and will not be able to connect to the real access point because of the de-authentication attack so the victim will probably choose the rogue access point because it has the same SSID as it shown in the figure 3.

Fig. 3 The victim is now connected to the rogue access point

The attacker will start using two primary tools (Wireshark tool, SSL Strip). Wireshark tool will make the attacker to sniff all network traffics, however there are many websites that provides SSL encryption to protect the users from sniffing and stealing confidential data, so the attacker will need to use SSL Strip [6] which is an MITM tool that is used to prevent the browser from upgrading to SSL encryption. Figure 4 shows a sample screenshot of Wireshark tool.

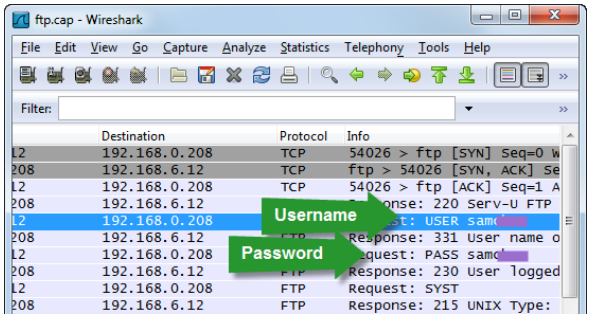

Fig. 4 Website password sniffing using Wireshark tool.

Evil Twin Attack is based on deceiving the victim with a fake access point. This can be done by adopting one of four popular attack scenarios.

3. Attack Scenarios

In order to eschew confusing we will refer the following four scenarios that the attacker can do to deceive the victims:

- Coexistence: The rogue access point and the victim's access point coexist at the same location. The rogue access point tries to capture victim's packets by providing a higher signal strength and has the ability to send a de-authentication packets to the victims that are currently associated with the certain access point.
- Replacement: The victim's access point is turned off physically and the name of the rogue access point has the same SSID.
- Ad Hoc Clone: The Attacker listens for probe requests, then the attacker will provide a rogue access point for the requested profiles by using a set of tools and a wireless device that supports monitor mode.
- Remote Clone: The rogue access point is sets in different locations. The rogue access point has the same name of the legitimate access point that is already saved in victim's profile and the victim will automatically connect to the rogue access point once the rogue access point discovered by the operating system of the victim. The figure 5 illustrates the mechanism of Coexistence attack.

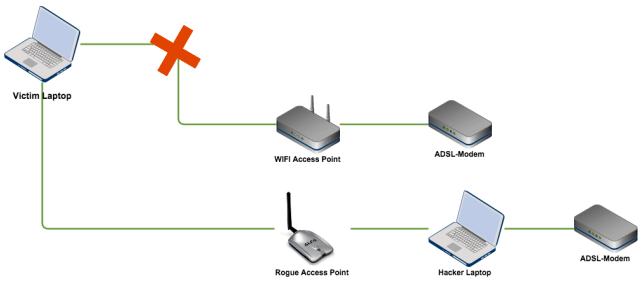

Fig. 5 Coexistence attack scenario.

To assess the threatening levels of these scenarios in reality, a field survey has been conducted mainly to gauge the awareness level of different types of common users.

4. Survey Methodology

The survey results are based on data that has been gathered from people living throughout Amman in 2015 as a part of research study on how to mitigate Evil Twin Attack in wireless 802.11 networks at Jordan by using convenience sampling method [6]. Convenience sampling "also called accidental sampling "is a type of non-probability sampling techniques which can be carry out with ease. Convenience sample will enable the researcher to gather a valuable information in a relatively fast and affordable procedures. This survey has been conducted getting use of Google Survey official form. The most essential feature of this form is the predefined multiple choice answers (Close Ended Questionnaires). To accelerate this process, physical attendance with the respondents has been carried out with so many groups in public places. One hundred people samples from Amman were randomly selected to participate in this survey. The respondents were given to complete this survey in English language. A total of 11 completed survey questionnaires were collected from each respondent. With this survey, we take into consideration the 4 attack scenarios that the attacker can do and how can we minimize the threat of this attack. The following topics may summarize the main methodology attributes.

4.1 Population Spectrum

Our sampling technique captured a good representation of gender, with 28% of respondents reporting female and 72% reporting male. In order to widen the survey spectrum, no specific age limit has been imposed or considered. Respondents ranged in age between 16-60 with median age of 20. This survey covered a wide spectrum of community elements with different education levels.15% of respondents completed high school, while 7% of respondents are diploma degree holders, 48% of respondents are bachelor's degree holders, 25% of respondents are master's degree holders, and 5% of respondents are PhD degree holders.

4.2 Risk Detection Measures

Being alerted from intangible risks is an unpleasant feeling. Knowledge and awareness are proven as the most effective weapons against such fears. In order to gauge this fact, the survey findings have been subjected to intensive analysis from different perspectives whereas main relevant topics such as Education Level, Fields of Interest, and Most Often Places were thoroughly addressed.

4.2.1 Awareness VS Education Level

The study concluded a proportional relationship between awareness level and education level as it shown in the figure 6. About 60% of PhD/M.Sc. holders were found frequent users of VPN in public places. On the other hand, only 20% of High School, Diploma, and B.Sc. holders were found educated enough to go with VPN in public places.

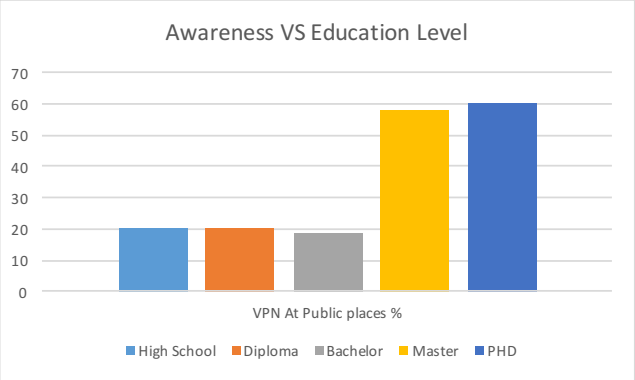

Fig. 6 Awareness VS Education Level

4.2.2 Anticipated Risk VS Field of Interest

The survey revealed the fact that Social Media websites are the most dominant among others. 50% of respondents were referring to social media relevant sites (Facebook, Twitter, Instagram, etc.) as the most favorite places they are interested in. On the other hand, 18% of respondents verified that their interest is mainly in exchanging emails, 14% surfing the web looking for a certain type of knowledge in specific fields,13% of them were so confident to use the web in money transfer actions, and finally only 5% of them used to verify their banking accounts through web. Figure 7 illustrates the field of interest percentages as demonstrated from the respondents.

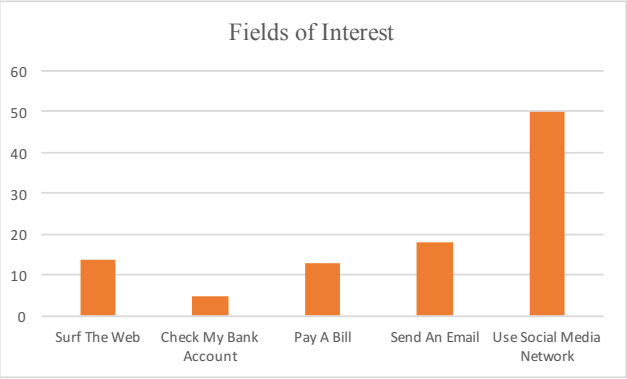

Fig. 7 Fields of interest percentages

It is obvious that Social Media is being found as the utmost type of exchanged data that may subjected to Evil Twin Attack risk among other types of information. On the other hand, checking bank accounts has been shown as the lowest dangerous field comparing to other fields of interests. The study depicted that those who are Bachelor/Diploma holders may be probable victims for Evil Twin Attack specifically while Paying Bills through public Wi-Fi networks. The attacker can easily use the Coexistence or replacement scenario in public places and has the ability to grab the credential data from the victim. Figure 8 illustrates further detailed information about risk field assessment per level of education.

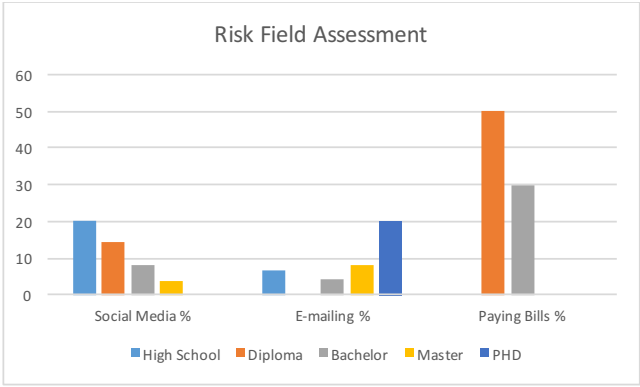

Fig. 8 Risk Field of Interest Assessment Based on Education Level

4.3 Most Often Places

Using internet at home practically offer 3 main advantages:

- Privacy
- Wider time range
- Low service prices

Accordingly, 45% of the respondents assigned Home as the most preferable place from their point of view. Work came in the second rank since most of work affairs are rely on internet applications nowadays. The rest common outdoor places such as (Coffee Shops, Libraries, Friend's Home, etc.) took less shares as shown in figure 9 with reasonable and logical percentages.

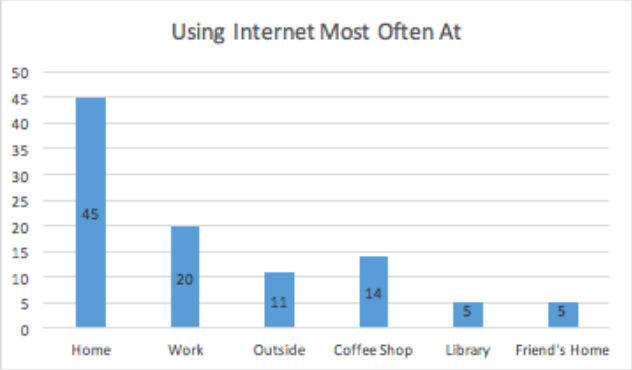

Fig. 9 Most often places

4.4 Risk Dashboard

If we consider Home, Work , and Friend's Home as a trustable places to use internet, and if we exclude web surfing from the risk list (as no valuable information can be eavesdropped by attackers is there),and if we dropped the "Checking my Bank Account" from the list since it has been rarely addressed by respondents; the following dashboard may represent a helpful visual aid that illustrates the anticipated risk degree per application for a spectrum of Non-VPN users with different education levels. Figure 10 illustrates the risk dashboard for Non-VPN users.

Risk Dashboard			
Degree	**Social Media %**	**E-mailing %**	**Paying Bills %**
High School	20%	7%	0%
Diploma	14%	0%	50%
Bachelor	8%	4%	30%
Master	4%	8%	0%
PHD	0%	20%	0%

Color Coding	
Range	**Status**
X≥20%	Critical
5%≤X<20%	Moderate
X<5%	Low

Fig. 10 Risk dashboard for non-VPN users

The following facts are concluded from the risk dashboard:

- High School and Teenage users are the less cautious users among others while sharing their personal information in social media sites. On the other hand, they showed no tangible interests in financial related activities and this is due to the modest financial capacity of this element.
- Diploma and Bachelor elements represent the mid field categories in this survey. They showed less interest in social media sites and higher interest rates in financial activities (Paying Bills). However, the survey revealed that this element maybe subjected to the ultimate level of threat due to their modest level of awareness.
- The survey revealed that those who have higher education's degree (PhD., M.Sc.) are the most cautious users among the other categories. They may trust the security measures of E-mailing sites but rarely share valuable personal information in social media sites and never jeopardize their money transactions processes without a protection.

5. Recommendations

There are existing solutions that the users should follow to get protected from this attack and users should know that the Anti-Virus and Firewalls are not enough to secure themselves from Evil Twin Attack. Anti-Virus is only a tool that is used for locate and delete computer viruses, Trojans, spyware and does not protect the users from hackers on a shared public network such as (Coffee Shop, Hotel, Airport lounge, etc.) only locates and deletes the computer viruses, Trojans, adware and spyware from computer. Firewalls are programs that control the inbound and outbound traffic and can only permit or deny communication. Both are necessary to prevent attacks but it will not protect transmitted data when you are connected to a public Wi-Fi network.

Rely upon HTTPS websites is a good way to protect the users from the attackers when they are connected to a public Wi-Fi network because it will create an encrypted link between the website and user's browser and will ensure that all data passed between them will be private. VPN which is stand for virtual private network is a great service that will help the users to protect their own data from hackers and their attacks. VPN will encrypt all the inbound and outbound data traffic of the user's computer or smartphone by using an encryption algorithm and key on both sides. This service will block the attackers from attempting to catch or modify any kind of data whether they set up a fake access point, aka the Evil Twin attack, using sniffers to read all inbound and outbound traffics, or using MITM attack. The table below illustrates the benefits of VPN.

Table 1. The benefits of VPN

Specifications	Internet without VPN	Internet with VPN
Enhanced Security	The data is not secured and not encrypted over the network.	The data is secured and encrypted over the network.
Online Anonymity	Users can be easily traced.	Surfing the web in complete anonymity.
Change IP Address	The IP address cannot be changed.	The IP address can be easily changed.
Privacy	There is no privacy at all.	There is privacy,
Unlock Websites	Users will not be able to access any blocked website	Users will be able to access any blocked website

Public places should start using VPN coupled with authentication to protect their costumers and mitigate the risk of these attacks by installing a third-party application such as FreeRadius [7]. When a costumer connects to a public Wi-Fi network in a coffee shop or any other public place a splash screen will pop up to the costumer asking for a username and password which can be required from coffee shop authorized person and in this way, the costumers will be reassure that are not connected to a rogue access point.

6. Related Work

As stated in the introduction public Wi-Fi network is extremely dangerous and it is vulnerable to man in the middle attack, Evil Twin attack, or eavesdropping. These papers exhibit the need for improving Wi-Fi network in public places. Some papers will show the behavior of people toward Wi-Fi network (802.11) in public places. Evil twin attack is one of the highest threats to public Wi-Fi networks [8]. Therefore, users must be educated on how to remain themselves secure when they are connected to a public Wi-Fi network by using VPN Services or any service that will make user's data secured. Polak and his colleagues presented an effortless mechanism that help the users to protect themselves from Evil Twin Attack in public places [9]. This method offers small authentication string protocols for trading cryptographic keys. The small string proof is discharged by encipher the small strings as a series of colors, transferred progressively by the user's device, and by the access point that belongs to the cafe or any other public place. Rachna Rajput et al, implemented a methodology simulating it using Matlab to detect and eliminate rogue access points to detect mac address spoofing of the authorized access point, prevent session hijacking and heartbeat monitoring by using sensor nodes and heartbeat monitoring methodology [10]. To compute the ratio of the threat of Evil Twin Attack, a study has been conducted on 92 respondents to collect their Wi-Fi usage patterns by Developing a context-based recognition algorithm that can help to reduce the threat of evil twin attack [11]. While it cannot prevent the attacks completely it gives users a high probability to detect them. Haitham Noman et al, has designed a De-authentication tool called "IJAM" written in python language [12]. This tool is used to disrupt the connection between the client and access point by sending a forged De-authentication packets by exploit a certain design flaw in wireless layer two protocol. Fabian Lanze and his colleagues provides a detailed summary about a set of tools that do not required some special skills and has been developed to make a rogue access point and unable the users to differentiate between the rogue AP and a legitimate AP. The researchers proposed a set of techniques that can be used to mitigate evil twin attack and to improve security for users of public Wi-Fi access points with minimal overhead [13]. Researchers from Daffodil International University have worked on an experimental analysis to study the known attacks related to IEEE 802.11 WLAN. The analysis and finding from this paper proved that the complexity of attacks has been increased by time and WLAN has become riskier to the users and business environments [14]. Researchers from Northeastern University presents a novel and very practical stealthy way that targets a large number of access points with WPA encryption to implement Evil Twin Attack and discuss the countermeasures that the users should do to protect themselves from these types of attack. The attack has been done on 17 technically sophisticated users and none of them were able to detect this type of stealthy attack [15]. Christian Szongott et al, sheds the light on how the new capabilities of smartphones can be used to create a rogue access point and show how easily can be used to create a mobile malware which is capable of spreading generally in metropolitan. This paper presents a proof of concept

implementation for IOS Devices and measured the key attributes of the MET [16]. Another Evil Twin Attack detection method that belongs to a group of researchers from University of Central Florida proposed a technique to detect Evil Twin Attack. This technique is a client side approach by using a different gateway compared with the gateway used by the genuine Wi-Fi hotspot. This technique was prototyped and evaluated using real scenarios. in addition, detection time is really short and time delay deviation does not influence the detection efficiency [17]. The last 10 years in the field of computer networks has become more critical to enterprises. Efficient security policies are designed to minimize the risk of attacks on Wi-Fi networks to ensure the confidentiality, integrity, and availability of data that pass through the network. The researchers have demonstrated a set of techniques that will help to secure networks. One of the techniques that has been used is developing an understanding of how WLANs can be hacked, and the mechanisms used to do same [18]. Harold Gonzales et al, proposed a set of defenses that will help to mitigate Evil Twin attack by presenting a methodology called context-leashing that requires Wi-Fi hotspot trust by location, design a session key establishment protocol that compatible with WLAN standard. Finally, to reduce the hazard of SSH Authentication, researchers presents a reporting protocol called “crowd-sourcing-based” that is used to provide historical information for the public keys of access points [19].

7. Conclusion

The potential of using a free Wi-Fi connection in public places combined with high risk for evil twin attack, imposed the need for higher security measures to be taken for protecting user’s credential information and their privacy. However, it seems that a good number of users neglect security in favor of a free internet connection. Users often fail to protect themselves when they are connected to public Wi-Fi network. some of the users believe that their own computer is secured because they are using Anti-Virus, Firewalls and so on. Users should raise their security awareness in order to protect their sensitive information from Evil Twin Attack. In this paper, we shed the light on using public Wi-Fi network and their risks in Jordan and found that a high percent of Wi-Fi users are not protecting themselves from Evil Twin Attack when they are connecting to public Wi-Fi networks, the paper also propose some recommendations that the user should follow concerning the security of Wi-Fi networks.

8. References

[1] IEEE 802.11™-2012 IEEE Standard for Information Technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[2] Tse, David, and Pramod Viswanath. Fundamentals of Wireless Communication. Cambridge: Cambridge University Press, 2005.

[3] Lyne, James. "How Safe Are London’s Wi-Fi Hotspots? See the Results of Our Warbiking Ride." Videblog post. SOPHOS. N.p., 30 Apr. 2014. https://blogs.sophos.com/2014/04/30/how-safe-are-londons-wi-fi-hotspots-see-the-results-of-our-warbiking-ride-video/

[4] Where the Wires End Study | Eirrus “ Xirrus, 2015 Accessed December 23,2016 https://www.xirrus.com/where-the-wires-end-study/

[5] Malenkovich, Serge. "Do You Use Free WiFi Hotspots? A Survey.” Web log post. Kaspersky Lab. Kaspersky, 20 Oct. 2012. Web. Accessed 24 Nov. 2016`. https://blog.kaspersky.com/do-you-use-freewifi-hotspots-a-survey/471/

[6] Convenience sampling Powell, Ronald R. (1997). Basic Research Methods for Librarians (3 ed.). p. 68. ISBN 1-5 6750-338-1

[7] The FreeRADIUS Project." FreeRADIUS: The World's Most Popular RADIUS Server. Accessed December 12, 2016. http://freeradius.org

[8] Phifer, Lisa. "Top Ten Wi-Fi Security Threats."Web log post. ESecurity Planet. N.p., 8 Mar. 2010. Web Accessed 19 Nov. 2016.
http://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-WiFi-SSecurity-Threats.htm

[9] Ra Roth, Volker, Wolfgang Polak, Eleanor Rieffel, and Thea Turner. "Simple and effective defense against evil twin access points." In Proceedings of the first ACM conference on Wireless. network security, pp. 220-235. ACM 2008

[10] Rajput, Rachna. "Detection of Fake Access Point in Wireless LAN Network." International Journal of Advanced Research in Computer Science and Software Engineering. 5, no. 9 (2015).

[11] Szongott, Christian, Michael Brenner, and Matthew Smith. "METDS-A Self-contained, Context-Based Detection System for Evil Twin Access Points.”.

[12] Noman, Haitham Ameen, Shahidan M.Abdullah, and Haydar Imad Mohammed. "An Automated Approach to Detect De-authentication and Disassociation Dos Attacks on Wireless 802.11 Networks.” International Journal of Computer Science Issues (IJCSI) 12, no.4 (2015): 107.

[13] Lanze, Fabian, Andriy Panchenko, Ignacio Ponce-Alcaide, and Thomas Engel. “Hacker’s Toolbox: Detecting Software -Based 802.11 Evil Twin Access Points." In 12th Annual IEEE Consumer Communications & Networking Conference. 2015.

[14] Waliullah, Md, A. B. M. Moniruzzaman, and Md Sadekur Rahman. "An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network." *International Journal of Future Generation Communication and Networking 8*, no. 1 (2015): 9-18.

[15] Cassola, Aldo, William K. Robertson, Engin Kirda, and Guevara Noubir. "A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication." In *NDSS*. 2013.
[16] Szongott, Christian, Benjamin Henne, and Matthew Smith. Mobile evil twin malnets–the worst of both worlds." In Cryptology and Network Security, pp. 126-141. Springer Berlin Heidelberg, 2012.
[17] Nakhila, Omar, Erich Dondyk, Muhammad Faisal Amjad, and Cliff Zou. "User-side Wi-Fi Evil Twin Attack detection using SSL/TCP protocols." *In Consumer Communications and Networking Conference (CCNC)*, *2015 12th Annual IEEE*, pp. 239-244. IEEE, 2015
[18] Olufon, Tope, Carlene EA Campbell, Stephen Hole, Kapilan Radhakrishnan, and Arya Sedigh. "Mitigating External Threats in Wireless Local Area Networks." *International Journal of Communication Networks and Information Security (IJCNIS)* 6, no. 3 (2014).
[19] Gonzales, Harold, Kevin Bauer, Janne Lindqvist, Damon McCoy, and Douglas Sicker. "Practical defenses for evil twin attacks in 802.11." *In Global Telecommunications Conference (GLOBECOM 2010),*
2010 IEEE, pp. 1-6. IEEE 2010.