Common Digital Evidences for Detection of Evil Twins in a Network

Zakariyya Hassan Abdullahi[1], Prabhsimran Singh Walia[2], Nidhi Sagarwal[3], Mohit Soni[4]

[1,2,3]*Computer Science and Engineering,*
Lovely Professional University, Phagwara, India

zakariyya.11816039@lpu.in

Abstract— **Wifi networks are everywhere today, beginning with houses, train stations, bus stops, workplaces, schools, etc. As mentioned by the Wi-Fi Alliance, Wifi carries more than half the world's files. In Germany, for example, 87 per cent of cell phone data is transmitted via Wifi. Across the planet, there are four billion WiFi systems in operation. 1.2 Exabytes of data is consumed via Wifi per month. Security is therefore an important feature for consumers. Despite the immense success, Wifi networks are prone to different kinds of threats. The free access nature of Wifi renders it vulnerable to the most popular attack on Wifi networks, the Evil Twin access point (AP). We must also ensure that sufficient steps are taken to discourage its impact and reduce it. Evil Twin is a kind of Rouge Access Point (RAP) that is very easy to create / deploy, but it is not so easy to detect. In this article, Researchers have shown numerous methods for identifying Evil Twin attacks and have carefully studied each significant pre-existing technique used for the same attack.**

Index Terms—Wireless-Fidelity (Wifi), Access Point (AP), Rouge,Access Point (RAP), MITM, Sniffing, Spoofing.

I. Introduction

One can't imagine a day without the internet nowadays. It has become an important component of our lives. The World Wide Web is the world's most powerful medium for global learning. It has increasingly become the most dominant means of offering access to internet services, doing business, running financial operations and much more. Wifi became the most commonly used method for transmitting data through air, as the use of wireless devices grew. The Wifi industry hit a milestone of 6.4 billion in 2011 and in the coming years, demand is projected to rise at a steady pace. Wifi is therefore very easy to set up, since it is very user-friendly to use. Cyber threats have been on the increase as well. Wifi network connectivity comes with different threats, such as Bad Twin, MITM (Man in the Middle), ARP (Address Resolution Protocol)

Spoofing, De-authentication attacks, Jamming attacks. Due to these flaws Wifi became an attractive target for attackers to compromise and to eavesdrop wireless client information. Nevertheless, there is one of most dominant attack on Wireless *the Evil Twin attack is known as Local Area Networks (WLANs). Evil Twin is a kind of Rouge Access Point,* also called Fishing Access Point [1], deployed by the attacker for malicious activities such as tracking Network Infrastructure, conducting Man in the Middle Attacks (MITMM), Attacks like jamming etc. It is possibly unlikely for a regular person to locate the Evil Twin on an open WiFi network. There is the same Service Set Identifier (SSID) in The Evil Twin, which is nothing but the network name to which the user wishes to connect. Typical Evil Twin needs two Wireless Adapters [2], one for internet connectivity and one for Evil Twin Access Point formation. Two scenarios are now here, first, when Evil Twin connects to the actual / legitimate access point to get internet access, and second, when it uses some other link, such as cell data, to get internet access or to use wireless connections other than the real access point. 802.11 is the wireless protocol used in wireless networks by the Institution of Electrical and Electronics Engineers (IEEE) and does not provide adequate protection protocols to prevent these kinds of attacks. Wireless systems connect to the access point with the strongest received signal strength indicator (RSSI) score, according to the 802.11 standard, when there are multiple access points with the same SSID in the vicinity of the device. So that's why, as it normally has better RSSI value than the actual one, several devices connect to Rouge Access Point. As all packets go via Rouge Access Point, this helps the attacker to intercept / sniff the data streaming between clients and servers.

The authors have organized this paper into five sections. Section II discusses the problem statement while Section III describes various other solutions that have been previously proposed to counter this problem of overview and outcomes of previous research and the related work. Section IV proposes a novel solution whereas Section V discusses the future scope.

II. Problem Statement

The use of Wi-Fi-enabled wireless devices is increasingly growing. By default, there is no such method for end users to ensure that they connect to a secure, real / legitimate access point. These machines are currently vulnerable to malicious access points set up by an intruder / attacker. One special version of these is known as the Evil Twins. Evil Twins are entry points that use separate artifices to intercept private traffic such as passwords and impersonate their accessibility, such as identity spoofing. There are no techniques that currently exist to identify Evil Twins, but usually need network operators to interfere, such as comparisons of Round-Trip Time, extra tracking systems that are expensive and have some drawbacks. Instead, we suggest a composite solution that can be used by integrating two-three side variables of client identification.

III. Related Work

There are no identification methods currently Exist for the Bad Twins suggested by Chao Yang, Yimin Song and Guofei Gu the researchers. This paper presents some that have been found to be effective. Any of these also use the conditions that we have laid down.

There is a detection method suggested in 2015 that uses Bad Twin detection TCP / SSL protocols. [Here, the author has abused the 3way] TCP handshake operates and used it to detect whether or not two APs are linked to the same gateway, because in the second case where attackers have their own internet, they are able to detect the Evil Twin [3].

[4] Focuses on deciding whether AP is based on software or hardware. The features of beacon frames and probe frames have been used in this study. In particular, mismatch was used in the TSF (Timing Synchronization Function) timestamps and their RMS (Root Mean Square) values were evaluated to locate outliers.

Researchers in [2] have an efficient algorithm for the identification of Evil Twins based on smartphone hotpot. In order to different between variables between Bad Twin and legal AP, they have used ISP and time delay parameters.

In Another approach [5], researchers have concluded to identify Evil Twins is to change the configuration of probe response frames and establish external databases at both customer and AP to store additional frame information. They suggested adding an additional field in the probe response frame, i.e. count, to retain an additional table on both the client side and the AP. These tables have been tested before connecting to an AP that the values are aligned and should be in good order with that of an AP.

Researchers have built a full-fledged method called ET Guard to classify Evil Twins [6]. On client computers, there is Exist applications that needs to be enabled to restrict them from linking to Evil Twins. Legitimate AP fingerprints are stored in the cloud servers and are periodically checked and accessed by the program installed on the computer. In the Et Guard, different modules such as Request Handler, Packet Handler, Extractor, etc. here also been provided.

Another approach to solve the problem of Evil Twin detection can be solved using the method described in [7]. Orthodox traceroute functionality was used by researchers and the TTL functionality of TCP was abused. Was also executed also execute on both the client and server side, as the attacker will adjust the TTL values to avoid Evil Twin from being detected.

As suggested in [8], on IDS (Intrusion Detection System) called DES (Discrete Event Systems) has been developed by IIT Bhilai researchers. The key concept here was to use retry bit, sequence number an, and association Key, association response frame fields sent to a client from an AP to identify Evil Twin on the network.[12]

Another strategy proposed by National Central University, Taiwan researchers in 2015 was to detect packet forwarding in packets to detect whether or not a packet is forwarded[9] from one AP to another. In scenario 1, where real AP was used for the Internet by Evil Twin, this would fix our problem. A tool called the Evil Twin detector was developed to detect APs of the same SSID using watch mode, catch packets, detect packet forwarding activity and then result in AP being an Evil Twin or not.

A real-time client-side method of detecting Bad Twin was suggested in the literature in [10]. For this, a dedicated server was set up so as to it maintains a table containing a packet sequence, wireless customer name, and the field of AP MAC address. After submitting the start packet, the wireless user moves arbitrarily to another AP channel and begins listening to the data packets received by the dedicated server for some time. [1] Believes that the Evil Twin is not so far from the true AP. An application is built by researchers based on RSSI against Evil Twin attacks (DRET), which can operate at regular intervals and can give warning if an evil access point is found. The technique used in this is that the real AP position is the same and cannot be modified, so Evil Twin will not place itself at that spot, so RSSI values for real AP would be the same and on Evil Twin can therefore be detected. Some of these processes involve some form of central storage to be handled by the administrator, resulting in increased overhead. Customer side detection mechanisms can also be favored, since they would be both easier and quicker than admin side detection mechanisms.

IV. Suggestive Solution

The Evil Twin can be divided into two simple scenarios:

1. When Evil Twin is related to the true / legitimate AP to supply its consumers with the internet.

2. If Evil Twin uses its own Internet service that may be cell data or a dedicated broadband connection. Fig 1 indicates the situations in both cases. The solution to Evil Twin identification would be different in both cases. Factors that we should discern between Bad Twin and the legal Access Point are:-

- Wifi configuration portal/Router’s web interface
- IP addresses provided by DHCP (Dynamic Host Configuration).
- Captive/Login portal for accessing internet
- Traceroute
- Wireshark/Airmon-ng
- Internet Service Provider (ISP)

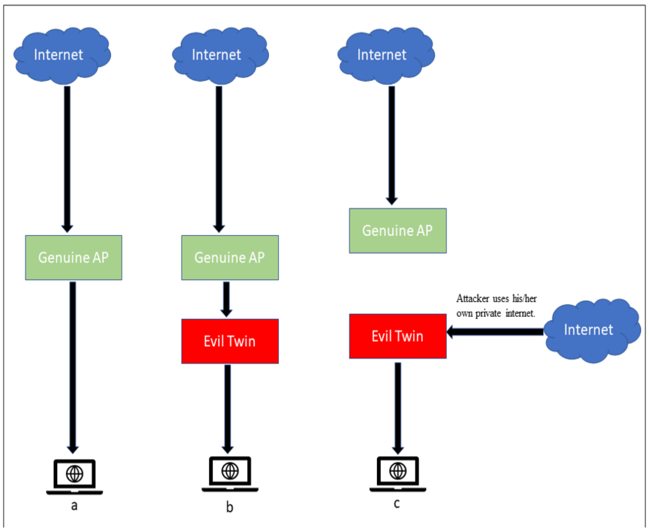

Fig. 1. Two Scenerios of Evil Twins 1.(b) and 2.(c)

1) *Web interface of the router:* Every wlan router has a web interface set up that allows different functionality such as port forwarding, status page (the status page indicates the current status and setup of the router. All data is read-only.), WPS settings, MAC filtering, DHCP configuration, parental controls, or IP and MAC linking, etc. This service runs on port 80 of tcp and can be accessed via the linked clients' default gateway address. As the Evil Twin might be using AP from various vendors, it will be different as that of legal one, even in the case of mobile hotspot, there will be no web gui at all because mobile phones do not accept this feature

2) *DHCP:* This service is used to provide each linked device on the network with IP addresses. In the absence of a DHCP server, an administrator must assign individual IP addresses manually to each and every host, which is a rather repetitive operation. DHCP encourages administrators to send clients a pool of IP addresses that can be allocated to them. This IP address pool is normally accessed after the network is sub netted and does not contain the gateway and broadcast address. In the case of Evil Twin, the ip pool will be different as the legal AP in the enterprise will have a subnet IP pool, which is not the case for Evil Twin.

3) *Captive Portal:* A captive portal is a website that is obligated to look at and travel with the user of a public-access network before access is given. Business hubs, malls, building lobbies, small outlets, and alternate venues that offer free Wi-Fi hot spots for net users are typically used by captive portals. These portals may contain various forms of methods of authentication, such as OTP (One Time Password), username and password, hidden key, etc. They are essentially used to ensure that only legitimate users are able to enter the internet from an access point. In Evil Twin there will be no or separate network interface portal for router setup as there will be version / vendor discrepancy between the evil AP and on legal are. Even in the event of mobile hotspot there will be no web interface at all because mobile phones do not support this feature.

4) *Traceroute:* It is a feature that displays the gateway address of each and every router that is between client and server. Three packets are sent to each hop present and their response time is measured. Basically, the traceroute utility uses the features of TTL (Time to Live) in packets, to know the number hops between transmissions. TTL is a maximum value that is set in each packet that is decremented by one as a packet passes through a router. When the client is linked to the Evil Twin, there will be an extra hop in the traceroute result.

5) *Airmon-ng:* Airmon-ng is a component of the Aircrack-ng utility script. It requires wireless interfaces to enable monitor mode. It is also used for going back to controlled mode from control mode. The packet sniffer, WEP and WPA / WPA2-PSK cracker, scanner and review platform for 802.11 wireless LANs are also included in the Aircrack-ng suite. It supports all network interface controllers with 802.11a, 802.11b and 802.11 g traffic sniffable drivers and supports the raw monitoring mode. In the case of Evil Twin of the same name and the same Mac address, there will be another AP in the vicinity.

6) *ISP:* The ISP is the internet provider which charges for flawless internet connectivity on a monthly / annual basis. If your internet connection has a problem or other technological fault is present, the ISP is responsible. ISPs may be industrial, nonprofit, operated by the government. The Evil Twin's ISP could be different. Clients should search their ISP and assume that they are not related to the actual APP. .

A. Situation 1

In this case Evil Twin is connected to real access point.

1) *Traceroute:* In first scenario there will be an additional hop with the legitimate AP in that traceroute result. So end user can distinguish that something is malicious.
2) *Captive Portal:* In first scenario Captive portal will be the same as that of real one, because Evil Twin is sharing the internet from the real AP.

B. Situation 2

In this case Evil Twin is using its own internet for providing internet to its clients.

1) *Traceroute:* In second scenario the number of hops will be less than that of first scenario as well than that of real AP, because here Evil Twin is directly connected to the internet and is having public ip, where as in second case there may be multiple routers within the organization routing the packets and typically there is only one gateway router in an organization which is present at the boundary of the network.
2) *Captive Portal:* In first scenario Captive portal will not be the same as that of real one, because Evil Twin is not sharing the internet from the real AP.

The bulk of the above-mentioned mechanisms make use of a single database, involving continuous maintenance. This all adds to additional overhead. There is no question that the use of multiple parameters for evil twin detection would improve the precision of detection, but the detection mechanism could be slow due to limited computing power and high memory consumption, as more processor cores and memory are needed to evaluate multiple parameters.

V. Conclusion

Several researchers have attempted to solve the Evil Twins issue in Wifi networks, but only for which recommended detection technique functions, all methodology needed prerequisites or standard circumstances. This paper suggests a single parameter to solve the above stated problem, but it is apt to say that one technique alone may not produce correct results in all the scenarios. It has been found that the proposed solution is stable, reliable and operates without predefined specifications. A hybrid approach to malicious twin identification is claimed to be capable of partake a lasting effect and give more accurate results.

References

[1] Z. Tang, Y. Zhao, L. Yang, S. Qi, D. Fang, X. Chen, X. Gong, and Z. Wang, “Exploiting wireless received signal strength indicators to detect evil-twin attacks in smart homes,” *Mobile Information Systems*, vol. 2017, 2017.

[2] H. Mustafa and W. Xu, “Cetad: Detecting evil twin access point attacks in wireless hotspots,” in *2014 IEEE Conference on Communications and Network Security*. IEEE, 2014, pp. 238–246.

[3] O. Nakhila, E. Dondyk, M. F. Amjad, and C. Zou, “User-side wi-fi evil twin attack detection using ssl/tcp protocols,” in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*. IEEE, 2015, pp. 239–244.

[4] F. Lanze, A. Panchenko, I. Ponce-Alcaide, and T. Engel, “Hacker’s toolbox: Detecting software-based 802.11 evil twin access points,” in *2015 12th annual IEEE consumer communications and networking conference (CCNC)*. IEEE, 2015, pp. 225–232.

[5] A. Kumar and P. Paul, “Security analysis and implementation of a simple method for prevention and detection against evil twin attack in ieee 802.11 wireless lan,” in *2016 international conference on computational techniques in information and communication technologies (ICCTICT)*. IEEE, 2016, pp. 176–181.

[6] V. Jain, V. Laxmi, M. S. Gaur, and M. Mosbah, “Etguard: Detecting d2d attacks using wireless evil twins,” *Computers & Security*, vol. 83, pp. 389–405, 2019.

[7] A. Burns, L.Wu, X.Du, and L.Zhu, “A novel traceroute-based detection scheme for wi-fi evil twin attacks,” in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[8] N. S. Selvarathinam, A. K. Dhar, and S. Biswas, “Evil twin attack detection using discrete event systems in ieee 802.11 wi-fi networks,” in *2019 27th Mediterranean Conference on Control and Automation (MED)*. IEEE, 2019, pp. 316–321.

[9] F.-H. Hsu, C.-S. Wang, Y.-L. Hsu, Y.-P. Cheng, and Y.-H. Hsneh, “A client-side detection mechanism for evil twins,” *Computers & Electrical Engineering*, vol. 59, pp. 76–85, 2017.

[10] O. Nakhila and C. Zou, “User-side wi-fi evil twin attack detection using random wireless channel monitoring,” in *MILCOM 2016-2016 IEEE Military Communications Conference*. IEEE, 2016, pp. 1243–1248.

[11] Liliana R. Horne. 2018. Development of a Client-Side Evil Twin Attack Detection System for Public Wi-Fi Hotspots based on Design Science Approach. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1064) https://nsuworks.nova.edu/gscis_etd/1064.

[12] Alberto Bartoli , Eric Medvet, Filippo Onesti Evil twins and WPA2 Enterprise: A coming security disaster.,” *Computer and security* 2018 Elsevier *s*, vol. 2

[13] P. Middleton, T. Tsai, M. Yamaji, A. Gupta, and D. Ruebe. (2017). Forecast: Internet of things – Endpoints and associated services. [Online]. Available: https:// www.gartner.com/doc/3840665/forecast-internet-things–endpoints