Fuzzy Systems and Soft Computing
ISSN : 1819-4362

TECHNIQUES FOR MITIGATING EVIL TWIN ATTACKS IN 802.11 NETWORKS

ASHOK KUMAR MISHRA
Raajdhani Engineering College, Bhubaneswar
[1]amishra@rec.ac.in

***Abstract*—** The 802.11 IEEE standard is being attacked via the Evil Twin Wi-Fi assault. The wireless connections are at risk due to the attack. The Evil Twin Wi-Fi assault is one of the more persistent types of attacks. After the Evil Twin Wi-Fi assault is carried out, it opens the door to a variety of further attacks, including IP spoofing, DNS spoofing, SSL stripping, and many more. For this reason, stopping the attack is crucial to data security and privacy. This essay will examine the attack's methodology in detail as well as various defense strategies. The suggested algorithm searches every channel for phony access points (APs) using the whitelist; if an unauthorized AP is found, *the user*

Keywords—Evil twin Wi-Fi attack; DNS spoofing; SSL strip; IP spoofing

I. INTRODUCTION

In today's world, wireless connections are becoming more important day by day. Almost all the appliance in use gets connected to the internet to customize, improve, and make our lives simpler, these devices are called the Internet of Things (IoT) [1]. The IoT protocol stack and some of the most used protocols and comparison of it from security aspect is discussed. Also, the paper attempts to present various challenges related to security from aspect of protocols, network, and device [2]. Various security gap in most of the current IoT technologies are reported [3-4]. The number of IoTdevices will be increase in future and it is important to find specific standard and mechanism to get security in the IoT [4].The majority of IoT devices use wireless connections to connect to the internet, this is usually IEEE 802.11 standard connection [5]. The IEEE 802.11 is specifically designed for wireless connections, the first 802.11 has been developed in 1997 and is still being improved on. This type of wireless standard is used with frequencies 2.4, 5, 60 GHz, the Evil TwinWi-Fi attack typically targets this standard [6-9]. To detect evil-twin attack, a real-time client-side detection technique is proposed [7]. A rogue Access Point (AP) detection technique based on the round-trip time (RTT) on the mobile-user side is proposed [8]. A Convolutional Neural Network (CNN) based Evil-Twin Attack (ETA) detection technique is proposed whichuses the preamble of the WiFi signal as the feature and uses it to train a CNN based classification model [9]. A novel ETS detection is proposed [10] which make use of the commonly used network diagnostic tool traceroute. A passive ETA detection scheme is proposed [11] by using channel state information in physical layer. a scan-based self anomaly detection (SSAD), which is a client-side solution to detect and mitigate channel-based man-in-the-middle attacks using access point (AP) scans [12-13]. Even though ETA is an old attack measure taken to prevent this attack is not common and is not implemented by a majority of the population. This attack is usually performed on public Wi-Fi networks where there are multiple users connected to the public network because it is open and multiple clients are connected to it, these types of networks make it a perfect candidate to initiate and perform the attack.

The attack begins with a dummy access point being created and fooling the client's device into thinking the fake access point is a better connection, this can be done either by increasing the signal strength of the connection or by disconnecting the client from the current access point (more on this later). The attack can also be performed in another way where the attacker sniffs the previously connected Wi-Fi connections and makes a fake access point with the same configurations, the device actively searches for previously connected access point and when it finds the fake access point with the same configuration as the legitimate access point the phone connects to the fake access point (AP). Once the device has connected to the attackers AP many man-in-the-middle attacks (MITM) [14] can be performed on this device to compromise the privacy and data security of the victim. In the below sections will be going through different methods to prevent such an attack and a custom method to counter this attack which includes the algorithm and the code explained in detail.

The detection and mitigation of evil twin attacks have recently received huge attention from researchers around the world. A virtual private network (VPN) is one solution available to counter-attack the evil twin attack but it is an inappropriate solution. In general, detecting the evil twin attack can be classified into two categories: client-based solutions [15, 16] and administrator-based solutions [17-18]. Although the majority of approaches being used belong to administrator-based mechanisms, they cannot detect evil twin in real-time and have a heavy overhead. A passive user-side solution, calledWi-Fi legal access point (AP) finder (LAF) is proposed in [19],to the notorious evil twin access point problem, which provide solution to various security problems. Discrete Event System (DES) based approach for Intrusion Detection System (IDS) for evil twin attacks in a Wi-Fi network is discussed [20].

Designing a client-side approach to detect evil twins is not easy for clients because users have limited resources and without an authorization list.

This work analyzes the feature of evil twin attacks and proposes a novel algorithm for mitigating the evil twin attack in a Wi-Fi network. Our scheme can make a deterministic and accurate decision on whether the client device is connecting to an evil twin AP. The implement and evaluate the proposed scheme with real experiments is done in this paper.

The organization of the paper is as follows. The various method of performing an Evil Twin Wi-Fi attack is reported Section II. The proposed system model and algorithmdiscussed in depth in Section III. The outcome of the proposed methodology is illustrated in Section IV followed by conclusion in Section V.

II. How does Evil Twin Wi-Fi Attack Work?

An evil twin is a fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications [1]. To perform this attack few to no additional hardware is required as shown in Fig. 1. In the test run a laptop with a wireless card (supports monitor mode). Alternatively, one can use a raspberry pi with a wireless card and a power bank to perform the attack remotely and discretely. For simplicity, it is recommended use premade tools such as airodump-ng, airbase-ng and aireplay-ng which can befound preinstalled in offensive operating systems such as Kali Linux, Parrot OS, and many more.

First set the card to monitor mode this can be done either through “iwconfig” or using the preinstalled tool called “airmon-ng”. Once the wireless card is in monitor mode then it can move to the next phase where it scans for the wireless connection, we want to perform the attack on. After obtain required information such as SSID, channel and other things, a malicious AP with the same configuration can be created.

Now there are two ways to do the next part one is to wait patiently for the victim’s device to connect to the attacker's AP or we use another method, which is a flaw in the 802.11b and some other standards where the management frames are not protected or validated. This method involves sending a crafted “Deauth frame” to the targeted AP as depicted in Fig. 2. The AP receives the frame and forwards it to the respective clients, the clients then receive the forwarded frame and are forced to disconnect from the targeted AP. The counterfeit access point may be given the same SSID and BSSID as a nearby Wi-Fi network.

The evil twin can be configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection [2]. What makes this attack so dangerous is that if a client does connect to this network intentionally or unintentionally, the client has no way of knowing that the device connected to the attacker's AP and his privacy and security is compromised.

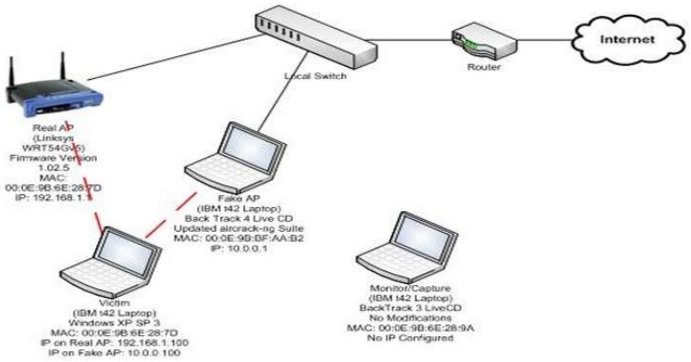

Fig. 1. Evil Twin Wi-Fi Attack Scenario.

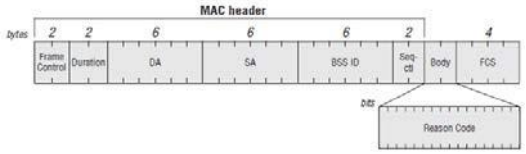

Fig. 2. Structure of Deauthentication Frame.

III. Proposed System Model and Algorithm

The proposed system in this paper is a counterattack against the Evil Twin Wi-Fi attack. The algorithm requires a list of known BSSID for whitelisting. The algorithm sniffs for fake AP using the whitelist in all the channels, once an unauthorized AP is detected the user has an option to de-authenticate any user in the unauthorized network in case any clients do connectto it by accident also the algorithm will be checking if any de-authentication frame is being sent to any of the AP to know which of the AP is being compromised. The program checks each channel for about 2 seconds and switches to the next channel also it scans for all 14 channels available in the 2.4GHz range.

As seen in Fig. 3, there is an Evil Twin Access point that is trying to mimic the actual access point. In Fig. 4, one of the victims connects to the evil twin, the counterattack then figures out which access point gets attacked and informs the Administrator about the attack. The administrator initiates the counterattack to disconnect the user from the Evil Twin Access point. First, the wireless card must set in monitor mode. Once the mode is set, then the whitelist, network name, and wireless interface as the arguments for the program needs to be provide. The program initiates by scanning networks in all the channels and finding any BSSID which is not in the whitelist this is done by checking all the wireless beacons. In the wireless beacon, check for its BSSID if the BSSID does not exist within our whitelist then mark it.

The program also checks if there is any deauth frame sent this similar to the whitelist where scanning of the wireless packets is done and we specifically check if the packet contains an 802.11 deauth frame, if it does this packet might indicate that the transmitter of the packet is the targeted AP. For the next step, a deauth packet is will send to the unauthorized AP and this is done by crafting a wireless deauth frame and specifying the transmitter address as target AP BSSID and deauth reason as 7. This program can be a good counterattack against unauthorized AP. It can be used with a raspberry pi and a wireless card and placed in separate locations. This can also be used to monitor wireless networks and can trigger an attack remotely.

The Fig. 5 is the complete flow of the code done in a flowchart. Here the scanning of channel for deauth frames and the quit command run in parallel this is to prevent any sort of interference to the code while scanning.

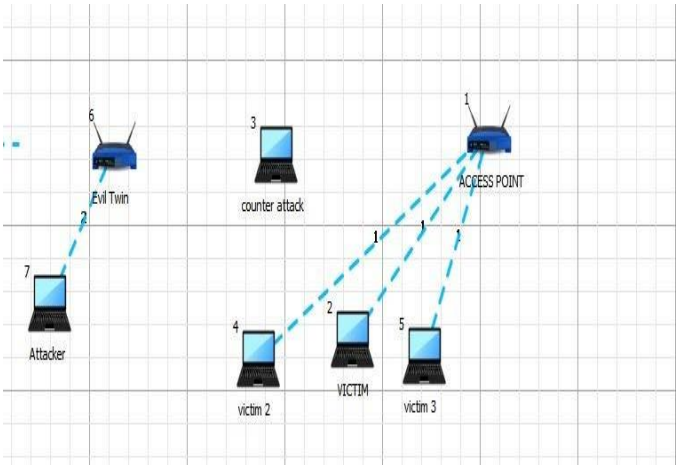

Fig. 3. Evil Twin Access Point which is trying to mimic the Actual Access Point.

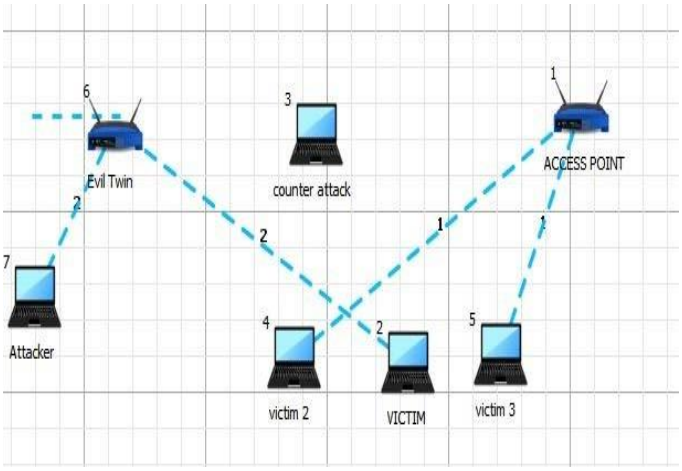

Fig. 4. One of the Victims Connects to the Evil Twin.

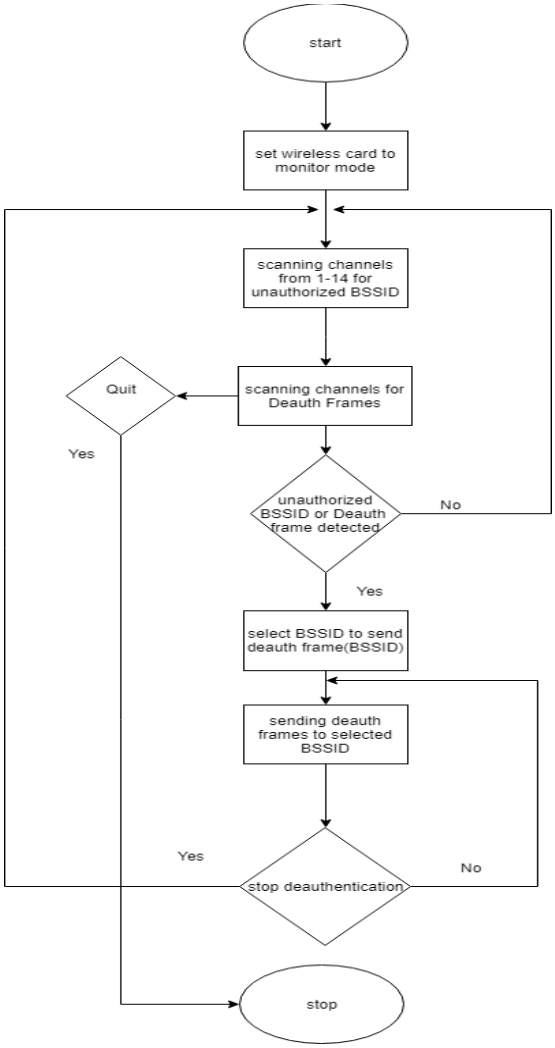

Fig. 5. Flow of the Code.

IV. Results and Discussions

This form of counterattack provides an easier interface and simplicity as opposed to manual methods. Also, it is compulsory to spread awareness of the attack, as more people know the attack less likely they fall for the attack. There are many other methods to mitigate this attack, for example using a virtual private network whenever connecting to an open Wi-Fi connection. Another method is by the new WPA3 standards which is released couple of months ago. This standard protects the wireless management frame thereby indirectly preventing the Evil Twin Wi-Fi attack.

In the above Fig. 6, one can see that only at higher education levels that the people are more informed about the attack. 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 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.

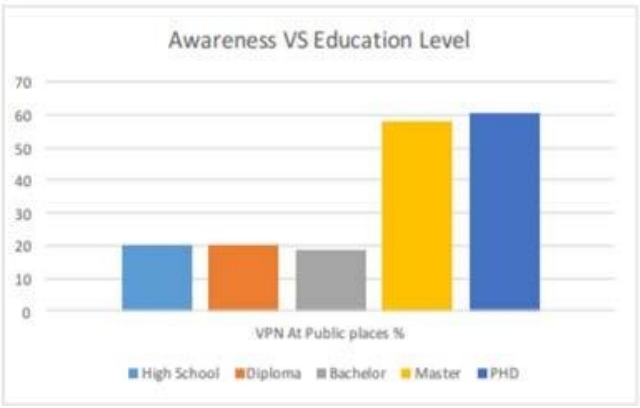

Fig. 6. Awareness Vs Education Level.

The study also showed that 58% of the survey respondents admitted using public Wi-Fi but only 7% had installed VPN service on their devices to protect their confidential data [3]. In conclusion Evil Twin Wi-Fi attack poses a serious threat to the users currently; therefore methods must be developed to prevent this attack. One of the methods which can be used to prevent such attacks is to use our proposed method where we can form an inexpensive method to counter the Evil Twin Wi-Fi attack.

V. CONCLUSION

There is always a network security threat that wireless users are vulnerable to be attacked by evil twins in WLANs so, in this paper, a novel approach to mitigating the evil twin attack to product wireless users from the hackers is proposed. The attack is simulated, and different measures are recommended toprevent the attack. The proposed algorithm sniffs for fake AP using the whitelist in all the channels, once an unauthorized APis detected the user has an option to de-authenticate any user in the unauthorized network in case any clients do connect to it by accident also the algorithm will be checking if any de-authentication frame is being sent to any of the AP to know which of the AP is being compromised. The efficiency of proposed approach is verified by simulating and mitigating the evil-twin attack.

REFERENCES

[1] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the Internet of Things: A Review," 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, , pp. 648-651, 2012.

[2] Sardeshmukh, H., & Ambawade, D. “Internet of Things: Existing protocols and technological challenges in security”. International Conference on Intelligent Computing and Control (I2C2), pp. 1-7., 2017.

[3] Sain, M., Kang, Y. J., & Lee, H. J. “Survey on security in Internet of Things: State of the art and challenges”. 19th International Conference on Advanced Communication Technology (ICACT), pp. 699-704, Feb. 2017.

[4] Yang Y., Wu L., Yin G., Li L., Zhao H. “A survey on security and privacy issues in internet-of-things” , IEEE Internet of Things Journal, vol.4, no.5 , pp. 1250-1258, 2017.

[5] N. Baghaei and R. Hunt, "IEEE 802.11 wireless LAN security performance using multiple clients," Proceedings. 2004 12th IEEE International Conference on Networks (ICON 2004) (IEEE Cat. No.04EX955), Singapore, pp. 299-303, 2004.

[6] O. Nakhila and C. Zou, "User-side Wi-Fi evil twin attack detection using random wireless channel monitoring," IEEE Military Communications Conference, Baltimore, MD, pp. 1243-1248, 2016.

[7] Yinghua Tian*, Sheng Wang and Long Zhang “Convolutional neural network based evil twin attack detection in WiFi networks” 2nd International Conference on Computer Science Communication and Network Security, 7 pages, Feb. 2021

[8] A. Burns, L. Wu, X. Du and L. Zhu, "A Novel Traceroute-Based Detection Scheme for Wi-Fi Evil Twin Attacks," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, pp. 1-6, 2017,

[9] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu. “A timing-based scheme for rogue ap detection”. IEEE Transactions on Parallel & Distributed Systems, vol. 22, no. 11 pp.1912–1925, 2011.

[10] C. D. Mano, A. Blaich, Q. Liao, Y. Jiang, D. A. Cieslak, D. C. Salyers, and A. Striegel. “Ripps: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network trafficconditioning”. ACM Transactions on Information & System Security, vol. 11, no. 2, pp-1-23, 2008.

[11] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. “Wireless device identification with radiometric signatures.” ACM International Conference on Mobile Computing and NETWORKING, pp. 116–127, 2008.

[12] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng. “Device fingerprinting to enhance wireless security using nonparametric bayesian method’ In INFOCOM, 2011 Proceedings IEEE, pp. 1404–1412, 2011.