International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2015): 3.791

Survey on Evil Twin Attack

Priyanka Sharma, Puneet Kumar Kaushal, Parth Rai Sharma

Abstract: ***During this present epoch use of Wi-Fi is not as secure as other networks principally in Public places akin to shopping complex, multiplex, coffee-shops, and university and so forth. Where there is an open access for Wi-Fi connection. Users essentially get attract towards the signal which provide high range, which may be a fake connection setup by an attacker to stole the private information of user. The target of attacker is to steal the personal data of victim such as username, password, credit numbers etc. But he is not able to copy the details of hardware details of an access points such as models, manufacture etc. Attacker setup the evil twin attack by installing it into his system by making same SSID he establish a rogue AP and enforce the victim to connect, by this he is able to accomplish his objective, after completing his objective he shut off the fake connection within a small duration of time. In this review paper we are describing a variety of techniques to detect and prevent from an evil twin attack. Because of some limitations of these previous techniques we are revealing our future approach to detect from this attack.***

Keywords: SSID, Evil Twin Attack, Wi-Fi, AP, Rogue.

1. Introduction

Today mobile devices are all around us and are now affecting everything we do in everyday life would be a somewhat minor statement to make, however constant growth in this popular area of technology can mean that it is sometimes efficient. If we think what's been going on and what will be the impact. If we jump back a trivial 10-12 years, we would be placed in an era where the majority of computers were still wired to a network with a trusty old Ethernet cable, and mobile phones were simply handy devices for making phone calls, playing snake and sending text messages are there. But according to the fast forward days we have powerful computers that can carry easily in our pockets boasting quad core processors and wireless network cards, some of the vehicles like cars that can connect to Wi-Fi, 3G and 4G networks, and tablets that will take care of most of our everyday work and respite needs.

With more and more organizations or societies adopting these devices every day it got thinking to us about how secure such devices can be because we all travel with our mobile devices, carry them everywhere with us where we use to travels most– By their very nature mobile devices present a number of immediate and interesting properties such as knowing which Wi-Fi networks they are connecting to when you are out? How accessible is the stored data once it has been stolen? What happens if the tool is misplaced or stolen?

But during recent years, Wireless networks are becoming very popular due to its wide range users can connect it via their mobile phone (smart-phones), laptops, tablets etc. They can connect to WiFi connections called “hotspot” in public as well as private area only difference is of security, you need wifi password before connecting at private places but there is an open connection to all the users at public places, no security or password is required, so the chances of fraud are more which is referred to as “Evil Twin Attack” [4]. Public places are like Airports, Hotels, Shopping points such as complex or malls etc.

There are some of the advantages of Wi-Fi such as people can stay online all the time or Wi-Fi also provide high speed, unlimited downloading or surfing’s or some provide limited data like data-packs in mobile phones.

An Evil Twin Attack some time called **“café latte attack”** because the attack mostly occurs at coffee-shops where a hacker gathers the information about an access point and then uses that information to set up his own system to use the real AP to mimic the access point. All users use their devices to connect to the access point but they are unaware of that they are actually connecting to the hacker’s system.

Researcher says Evil Twin Attack is kind of phishing, where users information is being captured by a hacker same Evil Twin works as rouge access point that appear to be original but in real it’s a fake one that is setup by a hacker itself to snoop on wireless communication between internet connections [14]. Once the user is connected to this fake wifi connection or rogue access point his/her all private information is lost. For example, once user has chosen to connect a particular network that is showing in his preferred list of network, when a client is searching for its preferred network a probe message is send by the client to its network list. This message is intercepts by an attacker and deploys an evil twin that offers the connection with same name (SSID) and high signal range. When a client sees a network in his/her chosen list it will connect automatically to this AP (rogue AP) which is an evil twin, by this attacker is able to steal victim’s personal information like passwords, credit card information etc. Hence, rogue AP act like an “evil twin” access point. This is the cause that while the wireless card notices other limited accessible wireless network, generally equipment like laptops or smart phones will prefer to hook up the AP that offers the highest Received Signal Strength Indication (RSSI). The attack is not easy to map out seeing as the attacker shut off the attack swiftly after getting success to his decided goals or can say the attack comes only for short duration of time.
Evil Twin is fake AP attack which make believe to be genuine access point or attract users to connect with it and this attack does not required but it can DoS the real APs. When users connect through this attack it redirect the traffic, filter the traffic and do a number of man-in-middle attacks.

Some secure networks are also available attacker can disrupt an existing connection by launching **DOS (denial-of-service)** attack and force the user to associate with it [17]. Like this evil twin can launch one of several attacks without the knowledge of client. When a user is coupled to rogue or spoofed AP the invader can intercepts the information of user/victim by transmitting the data or introducing the **man-in-middle** attack [17]. Now spiteful APs are clever to perform man-in-middle attack on unscripted traffic that mean data is capable of be modification and read or to hijack sessions.

Through all this process without any authentication method client do not know the IP/identity of its access point. So Researcher have IEEE 802.11 protocol which is an authentication mechanism within WPA or WEP to establish identity of access points of a kind that its set-up name - SSID and MAC address as - BSSID, but it requires some pre-shared secrets. IEEE 802.11 requests a principled authentication server to allow the wireless devices which is not well-situated at public places or huge amount of traveling users where users may not be known in advance.

It has been studied by some great researchers that evil twin is a kind of version of phishing in real world wireless networks. Evil Twin attack compiles a serious hazard to wireless LAN protection. Evil twins typically require the superior twin for Internet access. That is, to relay the communication an evil twin sit in the core of the victim host and the good twin or the wireless hops for a user to access internet enlarged from one to two. Thus to extend the coverage the genuine wireless provider may use wireless bridge and they don't modify the single hop physical layer wireless channel. According to the standard 802.11 protocol, researcher notices that as long as the invader follows the TCP protocol and the 802.11 standard and the increased delay introduce by one added wireless hop that cannot be ignored. So some algorithms are proposed to identify the evil twin by differentiate the one or two hop. These algorithms are named as TMM (Trained Mean Matching) or HDT (Hop Differentiating Technique).

2. Literature Review

Payal Bhatia, Christine Laurendeau and Michel Barbeau presents an method to detect a evil twin attack and reveal the truth teller and evil twin transmitter. For the detection of this attack 4-square antenna is placed on each receiver as in Fig 1.1. In result the method is intelligent to detect an attack for 100% when the transmitters are present in non-identical zones, but detects only 53% of the attacks in condition where the transmitters are available identical areas [13].

Yimin Song, Chao Yang, and Guofei Gu proposed two Algorithms TMM (Trained Mean Matching) and HDT (Hop Differentiating Technique). In TMM we observe sequence of IATs Server with higher prospect of matching the trained mean of two hop wireless. At the end we noticed that client uses two hop wireless networks to converse. We can collect IATs Server in one hop or two hops in training phase. Eventually we figure the mean and standard deviation of IATs Server in both hops and to vary the one-hop or two-hop determine the average.

TMM is based on training technique and in some situation this algorithm is very time consuming or not a practical approach for a user to attain a preliminary awareness. Due to these limitations we go for non-training based algorithm to detect the attacks- Hop Differentiating Technique. In this we use theoretical value rather than absolute value to detect the evil twin attack. HDT improves TMM by eliminating the training requirements and HDT is immutable to environment such as network saturation. In HDT threshold is computed as the SAIR (Server-to-AP IAT Ratio) boundary to evolve one-hop or two-hop. If the probability of upper bound SAIR exceeds the threshold results in normal AP scenario and the lower bound probability of SAIR exceeds the threshold results in evil twin AP scenario. HDT use the observed SAIR rather than IATs Server that TMM use to make the final decision [7].

Harold Gonzales, Kevin Bauer, Janne Lindqvist, Damon McCoy, Douglas Sicker proposed an evil twin detection approach known as Context-leashing and (Secure Shell) SSH- style authentication protocol. SSH yield a secure channel over an unsecured network. Basically use for authentication of passwords, files or message passing by using public key cryptography. It has ability to generate the pair of public-private key to encrypt the connection. Context-leashing provide a way to user to guard themselves from evil twin attack without be in need of a change in wireless infrastructure but this approach have some constraint that it do not provide authentication, integrity or privacy that can prevent data injection attack whereas SSH-style authentication can make out wireless network securely and to overcome the limits of SSH, crowd-sourcing mutual reporting protocol is needed to provide historical information on APs [9].

J.Saranya and V.Pugazhenthi present the UnMASK (Utilizing Neighbour Monitoring for Attack Mitigation) that weaken the several spoofing attackers or detect the malicious nodes in network Fig 1.1. But the drawback is malicious nodes create collision with compromised nodes. UnMASK is a framework and uses as a building block to inspect its neighbouring nodes communication.

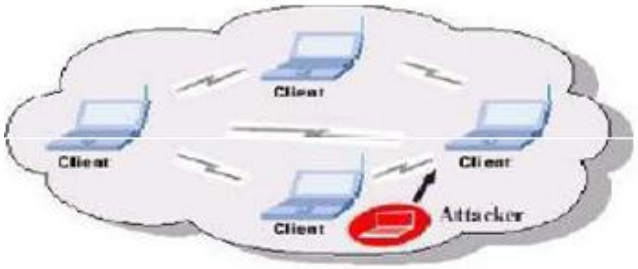

Figure 1.1: UnMASK

UnMASK is also used for securing the sensor networks because of its lightweight. (Link-state) LSR- secure routing protocol is build to provide protection against malicious nodes. LSR is use to create a graph of connected nodes in network to map which node is connected to which else nodes [8].

Aldo Cassola, William Robertson, Engin Kirda and Guevara Noubir proposed jamming techniques like use of software radios, trust models used in wireless authentication but have a downside that is difficult for users to detect it and is not able to work over 100m ranges [10] . In Reactive Jamming technique attacker jams a target in response to the wireless frames Fig 1.2.

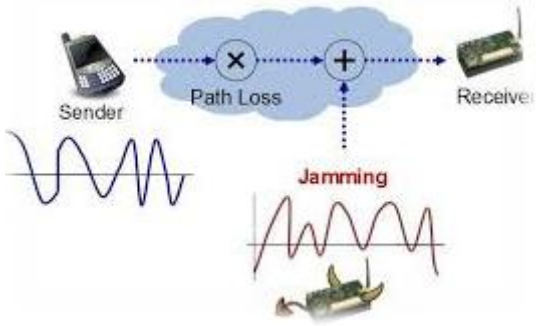

Figure 1.2: Jammer in Network

Before finishing the transmission of frames the attacker sends a Probe Request to jam the target. This approach works barely for fixed channel. In Deactive Jamming attacker sends fake packets unceasingly to jam the target and channel seems busy to original nodes [16].

Prabhash Dhyani present a statement how to increase the experience of Honeypot attack by recently discovered vulnerabilities of 802.11 and what remedies we can follow to protect from these Honeypot attack. Some of them are listed below:

- User should not accept the file which is untrusted.
- Clients should turn off the wireless interface, if the Wi-Fi is not in use.
- Clients should be configured [12].

Sachin R. Sonawane, Sandeep Vanjale, Dr. P.B.Mane proposed an approach of fake broadcast packet scheme to detect an evil twin attack in WLAN. The technique easily work on several type of network may it is wireless or wired but with a limitation that all the nodes should be in same subnet. Researcher technique does not work on different networks. Or if AP of attacker is not linked to the specify organization network then he won't be able to use the resources of organization network [11].

Chao Yang, Yimin Song and Guofei Gu, Member of IEEE proposed a solution for revealing of lightweight user-side evil twin attack their technique do not totally relay on "fingerprint" used for checking of deduce devices and this attracts the traveling users. They also propose statistical detection algorithm for evil twin detection i.e. HDT and TMM where HDT is best over TMM by removing the training requirements. Techniques are implemented in a prototype system - Evil Twin sniffer. After that they evaluate ETsniffer in respect to wireless networks, including 802.11b and 802.11g and output shows that ETsniffer can detect an evil twin fastly with good accuracy. Solutions are classified into two parts that is: First approach:-This approach is used to monitor the radio frequency (RF) airwaves or information that is gathered at routers and both are compared with the known authorized list of APs. Second approach:-This approach is used to monitor the traffic at wired side and check whether the machines use wireless or wired connections. These all approach are somehow limited because all requires the awareness of a list of authorized APs. So these solutions are considered as oppose to user oriented [1].

Fabian Lanze, Andriy Panchenko, Thomas Engel and Ignacio Ponce introduced differentiated attacker model as well as taxonomy for classifying countermeasures. They observed the problems that are still not solved and make possible them to put together their work. They also carry out a survey in this field to disclose the restrictions of state-of-the-art solution by using the aircracking suite software tool to increase the attack and introduced a novel scheme to sense the evil twin access point in which the attacker configure the fake Access Point with the help of software running on his/her device. But this approach is limited to only a specific tool which can be a problem further [3].

Kevin Bauer, Harold Gonzales, and Damon McCoy University of Colorado initiates two lines of defense averse to this attack. Firstly they present an ET detection approach called "context-leashing" based on nearby APs. By using this approach client determine whether a conflict has arranged an evil twin access point at a diverse location. Secondly they proposed an SSH- style authentication method known as "EAP-SWAT" that achieve one way access point authentication. These methods follow the standard of "trust-on-first-use". Also gives a mechanism to establish a shared secret key to create a secure session. In this approach no additional infrastructure is required. But one limitation of the trust-on-first-use strategy is it's apparently vulnerable to man-in-the-middle attack the first time the client contacts the service [4].

Maheshkumar Ramrao Gangasagare, May-2014 propose an approach of RTT (Round trip time) to distinguish between wireless and wired nodes. This information allows distinguishing between authorized APs, rogue APs and wired nodes. For the purpose of differentiating between wireless and wired node the higher variability and lower capacity in wireless network is used.

According to Mr. Gangasagare his approach not totally relies on training data nor depends on the type of wireless network. He proposed a detection approaches for evil twin attack in wireless network.

First approach keep an eye on Radio Frequency airwaves and further information gather at routers after that evaluate them with a recognized authorized list. However, this technique has the threat of fallaciously claiming a usual neighbour AP as a rogue AP.

Second approach monitors the traffic at a traffic aggregation position like gateway. It checks that the machine use wireless connections or wired. After this the information is compare by an authorized list to sense the AP is spoofed one. In short second approach solves the problem of falsely claiming by differentiate the customers whether come from wired or wireless network [5].

Sachin R. Sonawane, Sandeep P. Chavan and Ajeet A. Ghodeswar, October-2013 proposed (Rogue Access Point) RAP Detection Scheme Using Statistical Techniques**.** The objective of this method is to sense an evil twin attack in actual time under genuine wireless network. . However, this method planned two algorithms a learning free algorithm and learning based algorithm to notice an attack. These methods present two algorithms to sense evil twin attack which is Trained Mean Matching and Hop Differentiating Technique both employs the Sequential Probability Ratio Test Technique. Although RAP detection technique is not able to clearly identify rogue access point. TMM in some cases is time consuming and basically works for two-hops wireless channels as HDT use a theoretical value as SAIR value to tell between one-hop and two-hops SAIR [6].

Volker Roth, Wolfgang Polak and Eleanor Rieffel presents a protection mechanism towards an evil twin attack. User exchange public keys to secure their communication over the insecure channels. During this process two devices carry out their public keys and nonce which can be short consequently called "short authentication strings." Nonces are same if protocol proceeds without interference. The mechanism gives an advantage of exchanging cryptographic key for authentication protocols and the verification is performed by designated AP of café [14].

Diogo M´onica and Carlos Ribeiro proposed a client side device to become aware of an evil twin attack with its multi-hop characteristics. These tools are not dependent on any technology like latency or bandwidth of network and detect the attack in real time. The schemes do not involve the knowledge of an authorization list and is cost-effective tool. But have some problem they may identify a normal AP as fake AP [2].

S.No.	*Title*	*Methods/Approach*	*Result*
1.	Detecting and Localizing Transmitters in a Wireless Evil-Twin Attack	4- square antenna (to distinguish signals received from different angles– detect an attack) HPB-Hyperbolic Position Bounding (estimates the areas)	The algorithm is capable to perceive an attack for 100% when the transmitters are current in non-identical zones, but detect only 53% of the attacks in condition where the transmitters are available into identical area.
2.	Who Is Peeping at Your Passwords at Starbucks? – To Catch an Evil Twin Access Point	2 Algorithms – TMM and HDT	TMM is time-consuming or not a practical approach. HDT improve TMM through eliminating the training requirement. HDT is opposing to the situation change such as network diffusion.
3.	Practical Defenses for Evil Twin Attacks in 802.11	Context-leashing and SSH-style authentication protocol	Not support multiple APs and to ease the risk of trust-on-first-use model Collaborative reporting system is needed.
4.	A Practical, Targeted, and Stealthy Attack - Against WPA Enterprise Authentication	Jamming techniques	Can work at ranges under 100m only. Can't work up to 400m
5.	New Avatars of Honeypot Attacks on WiFi Networks	Resolving remedies for honeypot attack	Clients should turn off the wireless interface, if the Wifi is not in use.
6.	Mitigating Spoofing Attacks through Received Signal Strength in Wireless Networks	UnMASK (Utilizing Neighbor Monitoring for Attack Mitigation)	Malicious nodes form collision with compromised node.
7.	*Wireless LAN Intrusion Prevention System (WLIPS) for Evil Twin Access Points	Fake broadcast packets scheme	Won't work in network partitioning.
8.	Active User-side Evil Twin Access Point Detection Using Statistical Techniques	2 Algorithms – TMM and HDT and ETSniffer	Not sense all kind of man-in-the-middle attack in the WLAN
9.	Undesired Relatives: Protection Mechanisms Against The Evil Twin Attack in IEEE 802.11	Differentiated attacker model	Need large scale evaluation and limited to one specific software tool
10.	Mitigating Evil Twin Attacks in 802.11	Context-leashing, SSH-style authentication	Don't provide security for client session, vulnerable to man-in-the-middle attack
11.	Active User-Side Evil Twin Access Point Detection"	RTT (Round Trip Time)	Entail the knowledge of an authorization roll of APs or user.
12.	Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN	RAP Detection	Not able to clearly identify rogue access point.
13.	Simple and Effective Defense Against Evil Twin Access Points	Protection mechanism	Exchange cryptographic key for authentication protocols
14.	WiFiHop - Mitigating the Evil Twin Attack through Multi-hop Detection	Client side tool-Wifihop	May identify a ordinary AP as fakeAP.

3. Conclusion

In this paper, we have mentioned many techniques given by the researchers to detect the evil twin attack. Some of their techniques helped to protect from this attack but had their own limits such as they are not able to work over the range of 100m, not clearly classify rogue access point etc. Here we are proposing an approach to detect an evil twin attack and providing a mechanism of prevention through this attack. In our proposal we will use wireshark tool for capturing the packets on wireless network. After capturing the packets during both handshakes, we will manually analyze packets for legit as well as malicious AP.

References

[1] Chao Yang, Yimin Song, and Guofei Gu, 2012 "Active User-Side Evil Twin Access Point Detection Using Statistical Techniques", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.
[2] Diogo Monica and Carlos Ribeiro," WiFiHop – Mitigating the Evil Twin Attack through Multi-hop Detection", Institute Superior T´ecnico / INESC-ID Lisboa, Rua Alves Redol 9, sala 605, 1000-029, LISBOA.
[3] Fabian Lanze, Andriy Panchenko, Thomas Engel, Ignacio Ponce-Alcaide, Undesired Relatives:" Protection Mechanisms against the Evil Twin Attack in IEEE 802.11"
[4] Kevin Bauer, Harold Gonzales, and Damon, January-2009,"Mitigating Evil Twin Attacks in 802.11"
[5] Maheshkumar Ramrao Gangasagare, May-2014, "Active User-Side Evil Twin Access Point Detection", International Journal of Scientific & Engineering Research
[6] Sachin R. Sonawane *, Sandeep P. Chavan and Ajeet A. Ghodeswar, October 2013" Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN".
[7] Yimin Song, Chao Yang and Guofei Gu, "Who Is Peeping at Your Passwords at Starbucks? – To Catch an Evil Twin Access Point"
[8] J.Saranya, V. Pugazhenthi, July 2014, "Mitigating Spoofing Attacks through Received Signal Strength in Wireless Networks.
[9] Harold Gonzales, Kevin, Janne Lindqvist, Damon McCo, Douglas Sicker "Practical Defenses for Evil Twin Attacks in 802.11".
[10] Aldo Cassola William Robertson Engin Kirda Guevara Noubir Northeastern University, 2013, "A Practical, Targeted, and Stealthy Attack against WPA Enterprise Authentication"
[11] Sachin R. Sonawane, Sandeep Vanjale, Dr. P.B. Mane, April-June 2013, "Wireless LAN Intrusion Prevention System (WLIPS) for Evil Twin Access Points".
[12] Prabhash Dhyani, Wireless Security Researcher,Airtight Networks, "New Avatars of Honeypot Attacks on WiFi Networks".
[13] Payal Bhatia, Christine Laurendeau and Michel Barbeau, "Detecting and Localizing Transmitters in a Wireless Evil-Twin Attack".
[14] Volker Roth, Wolfgang Polak and Eleanor Rieffel, "Simple and Effective Defense Against Evil Twin Access Points"
[15] Jason Milletary," Technical Trends in Phishing Attacks".
[16] M.VamsiKrishna, R.Sudhakishore, November -2013, "Network Packet Jamming Detection and Prevention Using Hiding Method"
[17] N. Vijaya gopal, Dr.V.Srikanth, M. Mohan Chandra, 2013 "Survey on Different Types of Attacks and Counter Measures in Wireless Networks"