"Active User-Side Evil Twin Access Point Detection"

Mr. Maheshkumar Ramrao Gangasagare
Student of Master of Engineering,
C.S.E. Department,
M.P.G.I., School of Engineering, Nanded.

Under The Guidance of
Miss. Shital Y. Gaikwad
Assistant Lecturer,
C.S.E. Department,
M.P.G.I., School of Engineering, Nanded.

Abstract—Unauthorized or rogue access points (APs) produce security vulnerabilities in enterprise/campus networks by circumventing inherent security mechanisms. We propose to use the round trip time (RTT) of network traffic to distinguish between wired and wireless nodes. This information coupled with a standard wireless AP authorization policy allows the differentiation (at a central location) between wired nodes, authorized APs, and rogue APs. We show that the lower capacity and the higher variability in a wireless network can be used to effectively distinguish between wired and wireless nodes. Further, this detection is not dependent upon the wireless technology (802.11a, 802.11b, or 802.11g), is scalable, does not
contain the inefficiencies of current solutions, remains valid as the capacity of wired and wireless links increase, and is independent of the signal range of the rogue APs.

Our approach technically does not strictly rely on training data of target wireless networks, nor depend on the types of wireless networks. We propose to exploit fundamental communication structures and properties of such evil twin attacks in wireless networks and to design new active, statistical and anomaly detection algorithms. We can identify evil twins with a very high detection rate while maintaining a very low false positive rate.

Keywords— Rogue access point, wireless security, insider Threat, Evil twin attack, rogue AP detection, wireless security.

I. INTRODUCTION

Wireless networks are becoming extremely popular with the rapid advance of wireless LAN techniques and the wide deployment of Wi-Fi equipments. While users (especially smart phone users) can access Wi-Fi wireless internet "hotspot" connections in public more easily, they become more vulnerable to fraud and identity theft, referred as Evil Twin attacks. Evil twin is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers. Evil twin attacks, essentially a real-world wireless version of phishing scams, have been reported and studied by many security researchers. In previous year it found that security experts from Guardian launched two evil twin attacks conducted with volunteers, in which they successfully gather user's usernames, passwords, messages and even credit card information. This is mainly because many public Wi-Fi hotspots have no (or weak) forms of identification, except their Wi-Fi names (SSID), which can be easily impersonated.

We know there are too many travelling users accessing internet connection from wireless hotspot provided in public area. This may be possible that someone intentionally create rouge AP and provide internet access to them. As the traffic initiated from user goes through rouge AP, hacker

may analyze the packets and become successful in his intent of getting sensitive information of user. In existing solutions are administrators oriented and need much manual work. For example in large organization there is team of IT expert for searching rouge access point. They have sniffer software installed in their laptop and with some handhold devices to scan different frequencies which are not match with authorized one.

Figure 1: Illustration of launching an evil twin attack

An evil twin attack is easy to launch: As illustrated in Fig. 1, by using specific readily-available software, an attacker can simply configure a laptop to be a rogue access point (AP) to mimic the legitimate access point used in a free public Wi-Fi area. Such areas could be restaurants (e.g., MacDonald's), cafes (e.g., Starbucks), airport lounges, student community areas or hotel lobbies. Then, by physically setting the evil twin AP nearby the target victims, the rogue AP can attract the victims' wireless connections, either through passively waiting or actively sending dissociate frames to force victims to change connections. Then, by simply relaying victims' network packets between the attacker's rogue AP and the legitimated AP, the attacker can both provide Internet access to victims and steal victim's personal information, without the need of creating additional network connection channels to the Internet such as wired channels or 3G. In this way, the rogue AP essentially works as an "evil twin" AP.

An evil twin attack is easy to be successful: Since the "evil twin" AP is usually (physically) set closer to victims than the legitimate AP, the evil twin AP usually shows stronger wireless signal than the legitimate AP within the range of victims. Many end-users' laptops or smart phones may automatically connect to the "evil twin" AP with the highest signal strength among multiple APs associated with the same SSID. This is mainly because when the wireless card senses local available wireless networks, most operating systems of laptops or smartphones will choose to connect to the AP with the highest Received Signal Strength Indication (RSSI) for each unique SSID, as these operating systems believe different APs with the same SSID belong to the same organization.

An evil twin attack is hard to trace: since the attacker can shut off the attacks suddenly or randomly after achieving the malicious goals, leading to a very short time to detect. Through successfully launching such evil twin attacks, the attacker can intercept sensitive data such as passwords or credit card information by snooping at the communication links, or launching man-in-the-middle attacks as in the real-world experiments. The attacker can also manipulate DNS servers communications, control the routing, and launch more severe phishing or other attacks. In short, evil twin attacks compose a serious threat to wireless LAN security.

II. ROUGE ACCESS POINT DETECTION TECHNIQUES

Most existing evil twin detection solutions can be classified into two categories. All these below given solutions are administrative oriented.

The first kinds of approaches monitor Radio Frequency (RF) airwaves and/or additional

information gathered at routers/switches and then compare with a known authorized list. Most of technique scans RF from the Intranet APs to locate suspicious ones, and then compares specific "fingerprints" of the RF with an authorized list to verify. Specifically, for the scanning part, some techniques rely on sensors instead of sniffers to scan the RF, and some techniques such as propose a method to turn existing desktop computers into wireless sniffers to improve the efficiency. In this sensor for verifying certain frequency is distributed or placed in whole premises. For verification, these studies verify MAC addresses, SSID, and/or location information of the AP by using an authorized list. However, these solutions still have the risk of falsely claiming a normal neighbor AP as a rogue AP with a high probability. To solve this problem, they need to further verify whether such a rogue AP is indeed in the internal network. This can be done using a verifier to send packets to the wireless side. If such packets are received by the internal sensor, the associated AP is internal and thus an Evil Twin.

The second kind of approaches monitor traffic at the wired side (a traffic aggregation point such as a gateway), and determine whether a machine uses wired or wireless connections. Such information is further compared with an authorization list to detect if the associated AP is a rogue one. The second category of rogue AP detection solutions detect evil twins by differentiating whether clients come from wireless networks or wired networks, relying on the differences in diverse network protocols. If a client comes from a wireless network while it is not authorized to do so (comparing with an authorized list), the AP attached to this host is considered as a rogue AP. However, this line of work should solve the problem of falsely claiming an authorized wireless user who connects to Intranet with wireless networks.

These approaches are limited because they all require the knowledge of an authorization list of APs and/or users/hosts. We consider these solutions to be network administrator oriented, as opposed to user oriented. That is, they are designed for a wireless network administrator to perform authorization and access control policies for wireless APs/users. However, for a client user, it is of particular importance to be able to identify evil twins.

For example, traveling users who use wireless networks at airports, hotels, or cafes need to protect themselves from evil twin attacks (instead of relying on those wireless network providers, which typically may not provide strong security monitoring/management service). In addition, to protect wireless security, IEEE 802.1x protocol is also designed to provide a secured authentication mechanism for the wireless devices to connect to a LAN or WLAN. However, 802.1x needs an trustable authentication server to authorize the wireless devices, which may not be practical or convenient for the huge amount of traveling users to detect evil twin attacks by themselves in the most of current public areas. Thus, a lightweight, effective and user-side solution for these client users is highly desired but is currently missing.

User side evil twin detection techniques are TMM (Trained Mean Matching) and HDT (Hop Differentiating Technique) we will see in next chapters.

III. ACCESS POINT SCENARIOS

In this chapter we briey describe the topological deference between the normal AP scenario and evil twin AP scenario under our target evil twin attacks, which provides the intuition of our detection approach.

Normal Access Point Scenario

Figure 2: Normal Access Point Scenario

As illustrated in Fig. 2, under the normal AP scenario, a user communicates with the remote (DNS/Web) server through the normal AP (a one-hop wireless channel). There is only one path between normal access point and client and no in between them (hop) through which trace is forwarded. In normal access point scenario user is not victim of evil twin AP as user not sending network packet to evil twin even though evil twin AP present there. That means user accessing service of authentic AP.

Evil Twin Access Point Scenario

As illustrated in Fig. 2, under the evil twin AP scenario, the victim client communicates with the remote server through an evil twin AP and a normal AP (a two-hop wireless channel). As user forwards the network traffic through the evil twin AP, attacker by some way analyzes packet and get sensitive information of user. We have seen already attacker place AP with the help of his laptop and readily available software. This AP bears the same name (SSID) as authorized AP and creates confusion of user to which AP he should connect. Most of the time user gets connected to evil twin access point as it shows high RSSI (received signal strength). Most of the operating system considers the different AP bearing same name (SSID) is belong to same organization. In addition rouge AP shows higher signal strength as attacker place it nearer to victim. In such environment user get connected to rouge AP and become victim of evil twin attack. If user wants to know which AP is authentic and which is not that means user side detection of rouge AP is currently missing.

Thus, compared with the normal AP scenario, the evil twin AP scenario has one more wireless hop. This observation gives us the idea to detect evil twin attacks by differentiating one-hop and two-hop wireless channels from the user-side to the remote server. In next chapter we will see that introduction of one more hop can be distinguished as it require more time for packet to reach destination. To achieve our goal, we have to answer the following four questions:

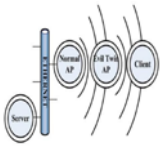

Figure 3: Evil Twin Access Point Scenario

What statistics can be used to distinguish one-hop and two-hop wireless channels on the user side?

Answer – IAT (Inter Packet Arrival Time)

Are there any dynamic factors in a real network environment that can act such statistics?

Answer - fluctuating RSSI, wireless n/w saturation

How to design robust and efficient detection algorithms with the considerations of these influencing factors?

Answer – TTM (Trained Mean Matching Algorithm), HDT (Hop Differentiating Technique)

What kinds of remote servers can be utilized to measure those statistics?

Answer - DNS server, web servers hosting local portal websites, public trustworthy servers such as “google.com”

In short, our paper makes the following contributions:

• We propose a new lightweight user-side evil twin detection solution. Our technique does not rely on

"fingerprint" checking of suspect devices nor require a known authorized AP/host list. Thus, this solution is particularly attractive to traveling users.

• We propose to exploit the intrinsic communication structure and property of evil twin attacks. Furthermore, we propose two statistical anomaly detection algorithms for evil twin detection, TMM and HDT. In particular, our HDT improves TMM by removing the training requirement. HDT is resistant to the environment change such as network saturation and RSSI fluctuation.

• We implement our techniques in a prototype system, ETSniffer (Evil Twin sniffer). We have extensively evaluated ETSniffer in several real-world wireless networks, including both 802.11b and 802.11g. Our evaluation results show that ETSniffer can detect an evil twin quickly and with high accuracy (a high detection rate and a low false positive rate).

IV. IMPROVEMENT BY DATA PREPROCESSING

We know that network is not always reliable and we are using the statistical analysis of (IAT) i.e. time distance between two successive packets arriving on client side. Due to high collision or from any reason time distance between some packet pair may be large. That means this data introduce noise and need to filter out. If we use such pair for analysis they may affect threshold which we are going to use for distinguishing two scenarios. In this section, we describe two data preprocessing techniques to improve the results: data filtering and data smoothing. For the first technique, we filter noisy data (according to the theoretical Server IAT) with a large number of network collisions. For the second technique, we use the mean of multiple input data, rather than only one collected data, to smooth the input.

(1)Data Filtering: With the considerations of some unexpected or unpredictable factors in the dynamic wireless networks, we also adopt data filtering policy to filter out those packets that may contain some errors. Specifically, in order to filter noisy data, we only consider the packets whose collision numbers may be at most three.(when the number of users is under 20, the probability that a packet has at most 3 collisions is over 85%). In this way, we can both filter the noisy data and keep sufficient data to implement the detection. Thus, according to the IEEE 802.11 standard and our filter policy, we filter out the packets whose AP IATs exceed 21,000 $_{us}$ or Server IAT exceed 39,800 $_{us}$.

(2) Data Smoothing: To further improve the result, we also use the mean of multiple input data rather than only one input data in one decision round. Specifically, we use the mean of multiple Server IATs or the mean of multiple SAIRs instead of only one Server IAT or one SAIR in one decision round to perform the threshold random walk. We name TMM algorithm and HDT algorithm using multiple Server IATs and multi SAIRs as multi-TMM algorithm and multi-HDT algorithm.

V. CONCLUSION

We can conclude that, above proposed solution for evil twin access point detection easily can be deployed on user side. Our solution work with less false positive and less false negative rate. The disadvantage of administrator oriented rouge access point detection gets easily removed because it does not need to maintain list of authorized access point. The interestingness of proposed solution is that it is more useful for the travelling user as it will not be feasible for administrator side to provide authentication for them. That means user will take care of himself without dependence on other. This technique can be deployed on user side so that user need not too much bothered about evil twin access point, it will get detected and come to know of user

when he trying to connect to rouge access point. We present two algorithms, TMM and HDT. They are helpful for detection of evil twin AP.

VI. ACKNOWLEDGEMENT

I am thankful to matoshri authorities giving me the chance to submit this paper "**Active User-Side Evil Twin Access Point Detection"** in the conference International Journal Sciences Engineering Research (IJSER). I am also thankful to **Miss. Shital Y. Gaikwad (**Assistant Lecturer at C.S.E. Department, M.P.G.I., School of Engineering, Nanded) giving me guidance to prepare this research paper. I offer my sincere appreciation for the learning opportunities provided by my committee.

My completion of this project could not have been accomplished without the support of my classmates, Akshay Chavan (Asst. Lect.), Saurabh Sawalkar, Premnath Kharat(Lect.), Nitin Kothwal, Rahul Natewad, Navinkumar – thank you for allowing me time away from you to research and publish.

Finally, to my caring, loving, and supportive father Dr. Ramrao N. Gangasagare (Principal at S.G.B.S.M., Purna) and mother: my deepest gratitude. Also, thanks to the brother and sister for their encouragement when the times got rough are much appreciated and duly noted. My heart full thanks.

REFERENCES

[1] Chao Yang, Yimin Song, and Guofei Gu, "Active User-Side Evil Twin Access Point Detection Using Statistical Tech-Niques" in *IEEE Information forensics and security*, vol. 7, no. 5, OCT- 2012

[2] L. Watkins, R. Beyah, and C. Corbett, "A passive approach to rogue access point detection," *in Proc. IEEE Globe-com'07,*Washington, DC,2007

[3] S. Jana and S. Kasera, On fast and accurate detection of unauthorized wireless access points using clock skews, *IEEE Trans. Mobile Comput.*, vol. 9, no. 3, pp. 449462, Mar. 2010

[4] L. Watkins, R. Beyah, and C. Corbett, "A passive approach to rogue access point detection*," in Proc. IEEE* Globecom'07,Washington, DC, 2007.

[5] C. Corbett, R. Beyah, and J. Copeland, "A passive a *IEEE Int. Conf. Communications (ICC'06)*, 2006, pp.

[6] A. Venkataraman and R. Beyah, "Rogue access po 802.11 MAC," *in Proc. Int. Conf. Security (SecureComm'09),*Athens,
Greece, 2009.

[7] J. Jung, E. Sit, H. Balakrishnan, and R. Morris, DNS

[8] K. Thompson, G. Miller, and R. Wilder, "Wide-area *Network, vol. 11, no. 6, pp.* 10–23, Nov./Dec. 1997.

[9] L. Ma, A. Teymorian, and X. Cheng, "A hybrid commodity wi-fi networks," *in Proc. IEEE Infocom'0*