Design of Recognition and Anticipation Rogue AP Using Similarity Safety Provision of AP

Nagesh Puri [1], Pratik Sarwade [2], Arati Sabane [3], Monika Waghole [4]

[1234] Student, Dept. Of CE, Sinhgad Institute of Technology, Maharashtra, India

Abstract- Wireless knowledge has been ahead rapid reputation for several years. The occurrence of insecure open 802.11 entrée points, it is presently easy for a nasty party to open a variety of attacks such as eavesdropping and data injection. In this paper, we judge a exacting risk called the evil twin attack, which occurs when an opposition clones an open access point and exploits universal routine access point selection techniques to trick a wireless client into associating with the malicious access point. According to a new study, 42% of wireless 802.11 access points give no security mechanisms — not even WEP or WPA. Wherever public Wi-Fi is presented is an occasion for an attacker to use that anxious hot spot to attack innocent victims. One detailed Wi-Fi hot spot attack called an "Evil Twin" access point can imitate any real Wi-Fi hot spot. Attackers will create sure their evil twin AP is now like the free hot spot association, and users are then duped when linking to an evil twin AP and the attacker can carry out frequent attacks to take improvement of the unacquainted victim. Wireless hotspots permit users to use Internet via Wi-Fi boundary, and many shops, cafés, parks, and airports supply free wireless hotspot services to magnetize clients. However, there is no endorsement system of Wi-Fi access points (APs) existing in such hotspots, which makes them helpless to evil twin AP attacks. Such attacks are injurious because they permit stealing responsive data from users.

We projected a new user-side evil twin recognition system that outperforms habitual administrator-side recognition methods in more than a few aspects. Different preceding approaches, it does not need a known approved AP/host list, thus it is more capable to recognize and avoid evil twin attack. Today, there is no client-side system that can successfully notice an evil twin AP attack so recover this problem using TMM and HDT detection algorithm.

Index Terms— Closed Evil Twin Attack, Rogue access point, AWS' S3, Scale-out, workload executor.

I. INTRODUCTION

WLAN Security knowledge has main use in lots of fields. Wireless LAN has a extensive range of applications due to its elasticity and simple entrée. The utilize of public Wi-Fi has reached at a point that is hard to avoid. Even as users can access Wi-Fi wireless internet "hotspot" connections in public more simply, they turn into to be more susceptible to deception and identity larceny, referred to as malicious attacks. The main stuff are what a lot of credentials in only client side or server side is defensive not the entire systems. So our solutions are detects malicious access points on the system using detection algorithm. We recommend a new lightweight server and client side malicious detection solution. Wireless technology allows a computer to be associated to a WLAN by means of "Access Points"(AP) through radio waves without the need for cables or wires. This allows several users to divide the same Wi-Fi1 AP or 'hotspot 'within a WLAN reporting range.

Over the preceding twelve years, 802.11 Wireless LAN's have developed and truly reshaped the network landscape. 802.11n is now quickly replacing Ethernet as the method of network access. The fast proliferations of mobile strategy has led to a fabulous need for wireless local area networks (WLAN), deployed in different types of locations, as well as homes, educational institutions, airports, business offices, government buildings, military facilities, coffee shops, book stores and many other venues. Besides, the services of elasticity and mobility of wireless devices has been concerned by most organizations and customers all over the world. Low price of hardware and user responsive system events allow anybody to set up their own wireless network exclusive of any professional knowledge of computer networks.

II. PROBLEM CONTEXT

In second section we explain our work briefly to set of some common points.

A. BACKGROUND

The majority demanding security issues that should be considered are Rogue Access Points (RAPs). A RAP is naturally referred to as a not permitted device which connects to the corporate network in many literatures. As the enlargement of mobile technologies, the order for communication over Wireless LANs System (WLANs) has improved. Additional and further users start to use wireless devices to access the Internet. On the other hand, the reputation of wireless communication also provides new opportunities to attackers. Wireless broadcast employs microwave to extend data over the atmosphere. So within the collection of Access Point (AP), all wireless strategy can accept the wireless indication. As the gesture can't be bound for to a particular recipient, it will be easy for cyber criminals to watch network traffic, disturb data flows and penetrate networks. These risks create wireless refuge to be more important.

Our main purpose is to provide simple, suitable, and functional techniques to moderate the threat posed by evil twin APs. To this conclusion, we first present an evil twin recognition policy that constrains AP hope by place. Then, we fight that wireless networks be recognized by public keys that can validate APs and bootstrap conference keys to secure data delivery.

B. EVIL TWIN RECOGNITION

An evil twin is a deceptive Wi-Fi access point that appears to be rightful, set up to listen in wireless communications.

When users log in to unsecured bank or e-mail accounts, the attacker intercepts the contract, since it is send during their apparatus. The attacker is also able to connect to additional networks.

Forged access points are put up by configuring a wireless card to operate as an access point (HostAP). They are tough to map out since they can be close off right away. The fake access point can be given the same SSID and BSSID as a close by Wi-Fi network. The evil twin may be configured to pass Internet traffic during to the valid access point while monitoring the victim's association or it can only say the scheme is provisionally occupied after obtaining a username and password.

B.1.1) RECOGNITION TECQNIQUES:

We implement two detection algorithms which are implemented in java technology with the help of packets .The packets are captured from Wireshark tools with all details of packets. The input of our algorithm is nothing but our packets which is stored into file.

B.1.a) Trained Mean Match (TMM)

The distributions of Server IAT in one-hop and two-hop wireless channels differs significantly. By use this figures, a recognition algorithm named Trained Mean Matching (TMM) is implemented. Specifically, specified a sequence of experiential Server IATs, if the mean of these Server IATs has a higher possibility of corresponding the trained mean of two-hop wireless channels, the projected method finish that the client uses two wireless network hops to commune with the remote server signifying a possible evil twin attack.

B.1.b) Hop Differentiating Technique (HDT)

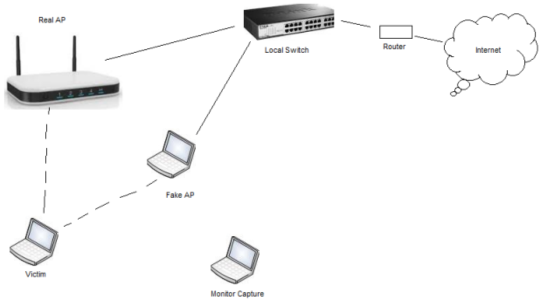
In TMM it uses the trained threshold, but immobile computes a hypothetical SAIR spring to differentiate these two scenarios. According to this examination, it develops a non-training based recognition algorithm named Hop Differentiating Technique (HDT) algorithm. Dissimilar from the TMM algorithm, in the HDT algorithm can use a hypothetical value for the threshold rather than a trained threshold to notice evil twin attacks. In the hypothetical multiplication phase, compute a threshold as the SAIR boundary to distinguish one-hop SAIR and two-hop SAIR.

B.1.c) Comparison of two algorithms

In this module, system will compare two different detection algorithms TMM and HDT to detect evil twin attack under different environment. To differentiate two algorithm with the help of execution time and average ratio.

C. System Architecture

The evil twin AP is an access point that looks and acts just like a legitimate AP and entices the end-user to connect to *our* access point. Our back track 5 r3 is flavor that can be used to make the fake AP which is first part of our implementation. This is a powerful client-side hack that will enable us to see all of the traffic from the client and conduct a man-in-the middle attack. Then we used Wireshark tool which is used to capture the packets from source to destination. The main goal is to detect the evil twin is completed by using IAT (Interval arrival time) find out. Wireshark shows the packets and their time as well as generate the graph. The original AP sending packet time is less so our IAT is also less, on the other hand fake AP packet sending time is large then its IAT is bigger than this is called fake AP. We implement the Two-Hop wireless connection means we have to implement evil-twin and their IAT is larger than one-Hop.



D.BLOCK DIGRAM

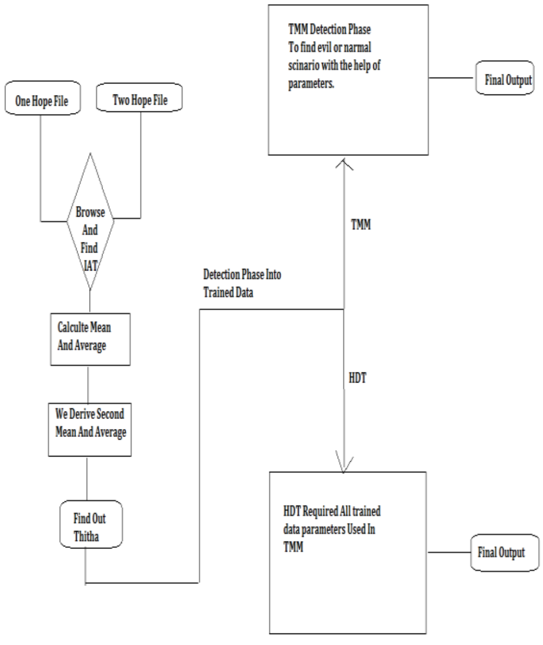


Fig. 1 Block Diagram Of TMM And HDT Algorithm

We Implement the TMM (Train Mean Match) & HDT (Hop Differentiate Technique) algorithms. We have to show One and Two hope wireless network fingers which is shown above block diagram.
Above Block diagram shows that how to go TMM and HDT for detection of Evil and Normal Scenario. Which is requiring to both one and two hope files which includes packets and time related to scenario? With the help of packets we calculate IAT and Average. Then we derive the second mean .Standard deviation is find out with the help of standard deviation formula.

Then probability find out which is similar to Tϴ values. We assign probability to approximately Tϴ value. And then Tϴ value decides which is evil tween or normal access point scenario.

The working of TMM and HDT algorithm is different but required input files and trained data is similar just some steps are different of HDT and TMM algorithm.

III. MATHEMATICAL EVOLUTIONS

We implemented our approach using Java development Kit. We have created the white list in that authorized clients are there. And compare their Internet Protocol (IP), SSID and MAC address then find out the unauthorized clients with the help of Wireshark toolkit and our formulas.

A. Equations and Implementation

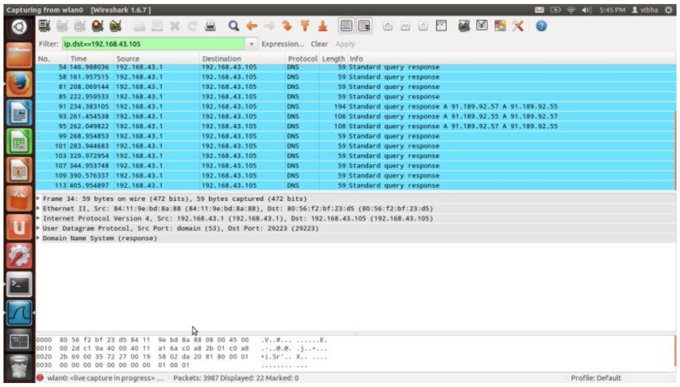
We collect Server IAT in both one-hop and two-hop wireless channels. Then, we compute the mean and the standard deviation of Server IAT collected in the one-hop (normal AP) scenario, with different variables. We are calculating the range with the help of range formula. Then we derive the second mean and calculate average of derive mean called as Tϴ. We obtain two probabilities of one Server IAT in these two scenarios exceeding the trained threshold, denoted as P1 and P2, by computing the percentage of collected Server IATs deviating from in the normal and evil twin AP scenario, respectively.

IAT is the intermediate packet arrival time of two consecutive packets. In this scenario, we have calculated IAT for one minute's packets and also calculate their average it is related to two hopes.

$$f(IAT)_{NAP} = \int_0^n (\text{Packets})_{\text{NAP}} \qquad (1)$$

Then IAT find out for two hope i.e evil tween access point is,

$$f(IAT)_{EAP} = \int_0^n (\text{Packets})_{\text{EAP}} \qquad (2)$$



```
Capturing from wlan0   [Wireshark 1.6.7 ]                                    5:45 PM  vibha
Filter: ip.dst==192.168.43.105                  Expression...  Clear  Apply
No.    Time        Source         Destination      Protocol Length Info
    54 146.988036  192.168.43.1   192.168.43.105   DNS          59 Standard query response
    58 161.957515  192.168.43.1   192.168.43.105   DNS          59 Standard query response
    81 208.069144  192.168.43.1   192.168.43.105   DNS          59 Standard query response
    85 222.959533  192.168.43.1   192.168.43.105   DNS          59 Standard query response
    91 234.383105  192.168.43.1   192.168.43.105   DNS         194 Standard query response A 91.189.92.57 A 91.189.92.55
    93 261.454538  192.168.43.1   192.168.43.105   DNS         108 Standard query response A 91.189.92.55 A 91.189.92.57
    95 262.049822  192.168.43.1   192.168.43.105   DNS         108 Standard query response A 91.189.92.57 A 91.189.92.55
    99 268.954853  192.168.43.1   192.168.43.105   DNS          59 Standard query response
   101 283.944683  192.168.43.1   192.168.43.105   DNS          59 Standard query response
   103 329.972954  192.168.43.1   192.168.43.105   DNS          59 Standard query response
   107 344.953748  192.168.43.1   192.168.43.105   DNS          59 Standard query response
   109 390.576337  192.168.43.1   192.168.43.105   DNS          59 Standard query response
   113 405.954897  192.168.43.1   192.168.43.105   DNS          59 Standard query response
▸ Frame 34: 59 bytes on wire (472 bits), 59 bytes captured (472 bits)
▸ Ethernet II, Src: 84:11:9e:bd:8a:88 (84:11:9e:bd:8a:88), Dst: 80:56:f2:bf:23:d5 (80:56:f2:bf:23:d5)
▸ Internet Protocol Version 4, Src: 192.168.43.1 (192.168.43.1), Dst: 192.168.43.105 (192.168.43.105)
▸ User Datagram Protocol, Src Port: domain (53), Dst Port: 29223 (29223)
▸ Domain Name System (response)

0000  80 56 f2 bf 23 d5 84 11  9e bd 8a 88 08 00 45 00   .V..#... ......E.
0010  00 2d c1 9a 40 00 40 11  a1 6a c0 a8 2b 01 c0 a8   .-..@.@. .j..+...
0020  2b 69 00 35 72 27 00 19  58 02 da 20 81 80 00 01   +i.5r'.. X.. ....
0030  00 00 00 00 00 00 00 00  01 00 01                  ........ ...
wlan0: <live capture in progress> ...  Packets: 3987 Displayed: 22 Marked: 0          Profile: Default
```

We are finding out delta and random variables from trained data which is derived from one and two hope files. Then Θ1 and Θ2 find out and P1 and P2 probability assign to Θ1 and Θ2.Whchi is normal and evil scenario. Then we are taken a one random variable which is 1 then we are says that evil tween scenario if random variable is 0 then normal access scenario.

$$f(T\Theta)=\frac{1}{2}\sum_{n=1}^{\infty}\left(f(IAT)_{NAP}+f(IAT)_{EAP}\right) \qquad (3)$$

Where $f(T$the set of average of IAT come from our equation (1) and (2).

IV. UNITS

Aircrack-ng is a network software group consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It mechanism with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic. Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured.

Total and average of packets are /sec which is captured from WiresharkToolkit.

TABLE I UNITS FOR MAGNETIC PROPERTIES

Symbol	EXPLANATION	Conversion from Second and Millisecond And Microsecond And Other
pf	packets frequency	2 Cycle/Sec→ 1 pack/Sec.
NAP	normal access point	1 Pack/Sec→Depend On wi-fi speed.
EAP	evil tween access point	1 Pack/Sec→ Double packet delivery ratio as compared original
P	probability	Probability assign to each T Θ value.
IAT	interval arrival time	1 Pack/sec →1000
PRO	protocol	against→user
DST	destination	1 Ope/Sec → dest address
-b	bssid	1 Ope/Sec= Original AP
-c	destination MAC address	1 = Wireless destination Interface
-h	source MAC address	1 Ope/Sec = Wireless source Interface
μ_{NAP}	normal access point avg	$\mu_{NAP}\rightarrow\mu_{snap}$
μ_{EAP}	evil access point avg	$\mu_{NAP}\rightarrow\mu_{seap}$
$T\Theta$	detection phase	1 Pack/Sec → NAP or EAP

Above tables shows all mathematical philosophy are used in development with their values.

V. CONCLUSION

We have to investigation network and there safety related issues using wire shark tool and backtrack operating system. A recognition algorithm named Trained Mean Matching (TMM). Particularly, known a series of experiential Server IATs, if the mean of these attendant IATs has a higher probability of matching the trained mean of two-hop wireless channels, we terminate that the client uses two wireless network hops to converse with the remote server representative a likely evil twin attack, and vice versa. Then we are used their results to implement TMM and HDT detection algorithm and their formulas. To Prevent and innovation against Evil Twin Attack in IEEE 802.11 Wireless LAN.

REFERENCES

[1] Chao Yang, Yimin Song, and Guofei Gu, Member, IEEE, “Active User-Side Evil Twin Access Point Detection Using Statistical Techniques”, IEEE Transactions On Information Forensics And Security, Vol. 7, No. 5, October 2012.

[2] H. Han, B. Sheng, C. Tan, Q. Li, and S. Lu, “A timing-based scheme for rogue AP detection,” IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 11, pp. 1912–1925, Nov. 2011.

[3] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko, “The one-more-rsa-inversion problems and the security of chaum’s blind signature scheme,” Journal of Cryptology, vol. 16, no. 3, pp. 185–215,
2003.

[4] Public wi-fi useage survey, Identity Theft Resource Center, 2012.

[5] A. Lamarca, Y. Chawathe, S. Consolvo, J. Hightower, I. Smith, J. Scott, T. Sohn, J. Howard, J. Hughes, F. Potter, J. Tabert, P. Powledge, G. Borriello, and B. Schilit, “Place Lab: Device positioning using radio
beacons in the wild,” in Pervasive, 2005.

[6] C. van Rijsbergen, Information Retrieval. 2nd ed. Butterworths, 1979.

[7] How to create an evil twin access point [Online]. Available: https://www.youtube.com/watch?v=LwEjYL6Eoro.

[8] Fake wireless access point creation-Rouge AP [Online]. Available: https://www.youtube.com/watch?v=CdqhNN1OfHY.

[9] Evil Twin in Wikipedia [Online]. Available: http://en.wikipedia.org/wiki/Evil twin (wireless networks).

[10] Ter Kah Leng, ―Wireless Internet regulation: Wireless Internet access and potential liabilities‖, Computer law & Security Report, Vol. 23 (2007), pp: 550 – 554.

[11] P.G.Sasane and S. K. Pathan, “Detection and Elimination of Fake Access Points in WLAN using Multi Agents and Clock Skew Methodology”, International Journal of Engineering Research & Technology, june-2014.

[12] K. Hole, E. Dyrnes, P. Thorsheim, P., “Securing Wi-Fi Networks”, IEEE Computer Society, 2005, vol. 38, no. 7, pp. 28-34.

[13] “Tired of Rogues: Solutions for Detecting and Eliminating Rogue Wireless Networks,” white paper, AirDefense, 2009.

[14]S. Shetty, M. Song, and L. Ma, Rogue Access Point Detection by Analyzing Network Traffic Characteristics, in Proc. MILCOM 2007, Orlando, Florida, October 2007.