Wireless LAN Intrusion Prevention System (WLIPS) for Evil Twin Access Points

[1]Sachin R. Sonawane, [2]Sandeep Vanjale, [3]Dr. P.B.Mane
[1]Dept. of Computer, BVDUCOE, Pune, Maharashtra, India
[2]BVDUCOE, Pune, Maharashtra, India
[3]AISSMS IOIT, Pune, Maharashtra, India

Abstract
Nowadays, Wireless Access Points are popularly used for the convenience of mobile users. The growing popularity of Wireless Local Network (WLAN) put forth different dangers of wireless security attacks. The vicinity of Evil Access Points is a standout amongst the most difficult system security concerns for system administrator. Evil Twin Access Points, if undetected, can take important information from the network. Numerous attackers took advantages of the undetected Evil Twin Access Points in ventures to not just get free Internet Access, and yet to view classified informative content. The vast majority of the present results for identify Evil Access Points are not automated and subject to a particular wireless technology. Undetected Evil Twin Access Point is one of the genuine dangers in wireless local area network since utilizing it; attacker can start MITM and Evil Twin attack on the users. In this paper, we have presented a new approach for detection of Evil Twin attack in WLAN. An Evil Twin is essentially a rogue Wi-Fi Access Point that looks like authorized AP.

Keywords
WLAN, RAP, Evil Twin

I. Introduction

WLAN technology has major use in numerous fields. Wireless LAN has an extensive variety of Applications because of its adaptability and straightforward Access. The utilization of open Wi-Fi has arrived at a level that is difficult to refrain. According to the poll conducted by Kaspersky's [8] global facebook pages 32 percent of the more than 1600 respondents said that they are using public Wi-Fi regardless of the security concerned. According to the JiWire report [9] in past year, total Wi-Fi usage has been doubled, increasing by more than 240% since Q2, 2011. It also specify that this rise is being due to the mobile devices and laptops account for just 48% of the connected devices. Depend on these two survey results, more educational awareness is necessary. Public Wi-Fi networks like at Coffee shop, Airports and so forth., are open for clients and for hackers, who are searching for touchy client information. Hackers can create Evil Twin access points in such places to steal such information. Evil Twin access point is a standout amongst the most genuine threats in WLAN today.

To address the shortcomings of existing solutions we have proposed Intrusion Prevention System (IPS) that automatically detects Evil Twin access points on the network and block them. In large networks such as university campus, enterprise, etc., it is very difficult for network administrator to manually detect Evil Twin access points and locate Evil Twin access points to remove them from the network. Hence, it is necessary to have automated intrusion prevention system, that not only detects Evil Twin access points but also block them. Thus making it easier to protect network from the threats of Evil Twin access points.

Our main contributions are as follows:

- We examined and analyzed different types of techniques to detect rogue Access Points.
- We proposed an approach to efficiently detect and block Evil Access Points on the network.
- We implemented a prototype of our approach and evaluated it by injecting several Evil Access Points in our wireless LAN. Our results showed that our approach is effective in detecting Evil Access Points on wireless network.

II. Background

Various security mechanisms are necessary in order to avoid threats against Wireless Local Networks. Different threats are exist on the Wireless Network; one of such serious threat is Evil Twin Access Point.

An Evil Twin attack is quick and easy to set as shown in fig. 1, attacker can easily set Evil access point and looks like the authorized access point used in public Wi-Fi area, these area could be coffee shop, restaurants, airtoprt...etc. Attacker can set up Evil access point near to the victims, the Evil access point then try to attack the victim's wireless connection by using different methods and force victim to change the connection. Generally Evil AP uses powerful wireless signals then the authorized AP inside the range. User's laptop or other device then automatically get connected to the AP with highest RSSI. Once victim is connected to the Evil AP, by catching network packets between Evil AP and the authorize AP the attacker can provide internet access and can get sensitive information similar to passwords, credit and debit card details..etc. In this way Evil AP works as an "Evil Twin" AP between victim and the authorize AP. the attacker can bring out more serious attacks like phishing. In short, Evil Twin attack is a dangerous threat to the WLAN Security.

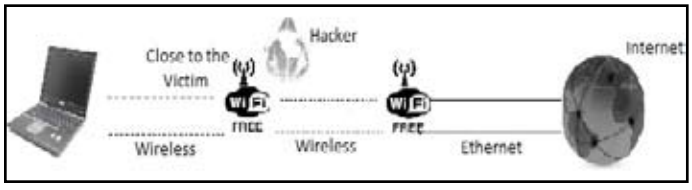


Fig. 1: Evil Twin Attack

III. Related Work

The threat of Evil Twin AP have attracted both industrial and academic researchers to focus on this problem. There are some methods presented which deal with this problem.

Hao Han and his colleagues used timing based scheme for Evil AP detection, [1] in that they have functional timing based plan for the client to avoid from connecting with Evil Ap. In their discovery system they have utilized timing informative content dependent upon the round trek time. Thought is to client test a server in neighbourhood and after that measure the RTT from the reaction, this methodology is rehashed number of times and all RTTs are recorded. Provided that the mean worth of RTTs is bigger than a fixed threshold, they acknowledge the partnered AP as an Evil AP. They have acknowledge four elements that have impact on timing RTT which are Data transmission rate, Location of DNS server, Wireless movement and APs workload. They have

tried precision of their method recognizing distinctive situations for these four components.

Taebeom Kim and his colleagues utilized received signal strengths for discovery of fake Access Point [2], in this they measures corresponded RSS arrangements from adjacent APs keeping in mind the end goal to figure out if the sequences are honest or fake. This system works in three stages. In stage one they are gathering RSS from adjacent AP, in Second Phase they are doing standardization of gathered RSSs, it assesses some missed RSSs, caused by some outside variables and standardizes the evaluated RSSs for generalization of an assortment of wireless environments. In third stage they are figuring out which RSSs are greatly corresponded to others dependent upon some empirical threshold value. They outline that remarkably associated RSS sequences as fake signals from a single device.

Qu and Nefcy presented new indirect Evil Twin Access Point detection system. [3] They broke down local round trip time(LRTT) information and composed a system with numerous calculations for identifying wireless hosts effectively. Their work begins from inactively examining or observing system movement to have disclosure and catching Client-side solution for Evil Twin Access Point.

Roth et al, put forth a modest assurance mechanisms that help the clients or customers to locate an Evil Twin openly Internet networks.[4] This technique gives short verification string protocols for trading cryptographic keys. the little string proof is executed utilizing encoding the short strings as an arrangement of colors, carried out consecutively by the client's device and by the specific Access Point.

Chao Yang and his colleagues have utilized Statistical method dependent upon TCP packets to figure their IAT to locate Evil Twin AP[5]. Assuming that customer is associated with remote server through Evil Twin AP and a standard AP that is two-hop remote channel, so this gives the thought to discover Evil Twin attacks by differentiating one-hop and two-hop remote channels from the client to the remote server. In this they have utilized two calculations, first is Trained Mean Matching, in this they are utilizing preparing method to distinguish Evil Twin attack. The second calculation is Hop Differentiating Technique; it is a non-preparing-based location calculation in which they are utilizing specific speculative worth for the limit to distinguish Evil Twin attack. They have tried this strategy under diverse RSSI levels for the correctness of the recognition of Evil Twin AP.

IV. Our Analysis

A. Design

In this section we will explain our problem statement and approach. Our solution will work on any type of network that is wired network, wireless network or heterogeneous network but only the constraint is all the nodes must be in the same subnet. There are three types of packets normally float on the network unicast, broadcast, and multicast. Unicast packet contains specific MAC address so it can be accepted by the host having specified MAC address and rest all host will reject the packet. Broadcast packet is a packet in which all the bits of MAC address are one and this packet will be accepted by all the hosts on the network. Multicast packet is a packet having multicast MAC address and each host on the network is having its own multicast MAC address list so when host receives any packet it checks the destination MAC address with its multicast list and if any entry matches with the destination MAC address then it accepts the packet otherwise the packet is rejected. Other than this there are special hardware addresses like in case of broadcast we make all the bits of MAC address one but here we will make all the bits one except first bit which we will keep zero. This is called fake broadcast. As all the bits are not one it is not broadcast address so all the hosts on the network will reject this packet. But we have observed that Access Points are accepting such packets.

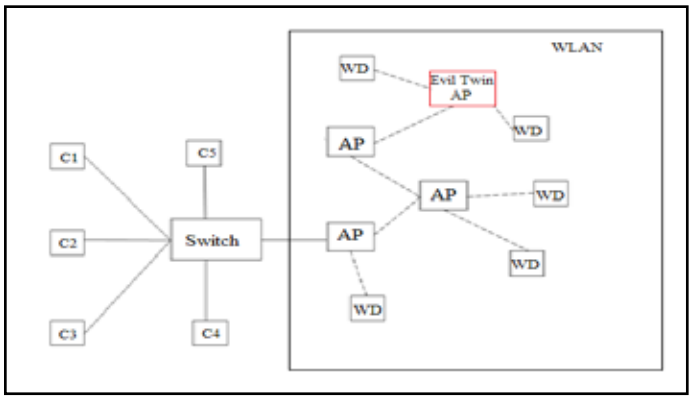
B. Features of the Solution

- Accurate Detection of Evil Twin AP.
- Less time to detect Evil Twin AP (2 to 3 ms).
- Scalable Solution.
- Consume very less bandwidth of the network.
- Apart from Detection of Evil Twin AP, help Administrator with Maintenance of AP.

C. Evil Twin access Point Detection Mechanism

Packets with all MAC address bits 1 excluding first bit is called Fake Broadcast address (i.e. FF:FF:FF:FF:FF:FE) and is rejected by all the network interface cards (NIC). But wireless Access Points accept this packets and reply to this packet as well. We are storing the list of authorized Access Points in the database as their IP address and MAC address. Then we are sending ICMP fake broadcast packet on the network and we will capture their reply. We have observed that we will get replies only from Access Points. We will capture these replies and check their IP addresses and MAC addresses with the authorized Access Point list we have with us. If it does not match, then definitely it is unauthorized Access Point otherwise it is authorized Access Point. Once the rogue Access Point is detected the same can be intimated to the administrator for any further action. As we are sending only one ICMP request packet on the network and all of the hosts are going to discard the packet and only Access Points are going to reply with again only one ICMP reply packet the traffic will not be increased much with this technique.

D. System Architecture



C1..N Desktop Computers, AP: Access Point, WD: Wireless Devices

Fig. 2: System Architecture

E. Implementation.

We implemented our approach using Java SE development Kit and Net Beans IDE v7.3. We used Jpcap library to capture packets and send ICMP packets to detect as well as block Evil Twin Access Points . Jpcap is an open source library for capturing and sending network packets from Java applications. We evaluated the prototype of our approach on a computer with an Intel Core 2 Duo 2.58GHz CPU and 4GB RAM, running Windows 7.We

have used Four Access Points.

F. Algorithm

Input: ICMP Packet,
Output: IP and MAC address of Evil Twin AP
Begin
Select ICMP Packet;
Set Destination ID as Subnet ID;
Set Destination MAC as fake broadcast address;
Use Broadcast IP address to broadcast packet on the Network;
If access points received packets then they reply to it;
Compare Reply packets (IP and MAC) with authorize list;
If a IP and Mac from a reply packet does not match with the Authorise list then go to step 8, else go to step 9;
Send alert message with details to the system and block Evil Twin AP by sending spoofed ICMP broadcast packet with Evil Twin's IP to cause smurf attack on detected Evil Twin access point;
If Reply equal to Authorise list;
Do nothing;
Display message Evil Twin is not present;
Repeat procedure after 30 sec
End.

G. Results of Our Solution

This software is being tested with 4 Access Points with 1 Access Point as rogue Access Point and 3 Access Points as authorized Access Points.

1. If Check AP button is ticked then it will get the existing Access Points information like IP address and MAC address on the network and check with the authorized Access Points IP address and MAC address information stored in XML file if any IP address is not in the XML file then it will consider it as rogue Access Point. It will display authorized Access Points in Authorized AP window and unauthorized Access Points in Unauthorized AP window (fig. 3).

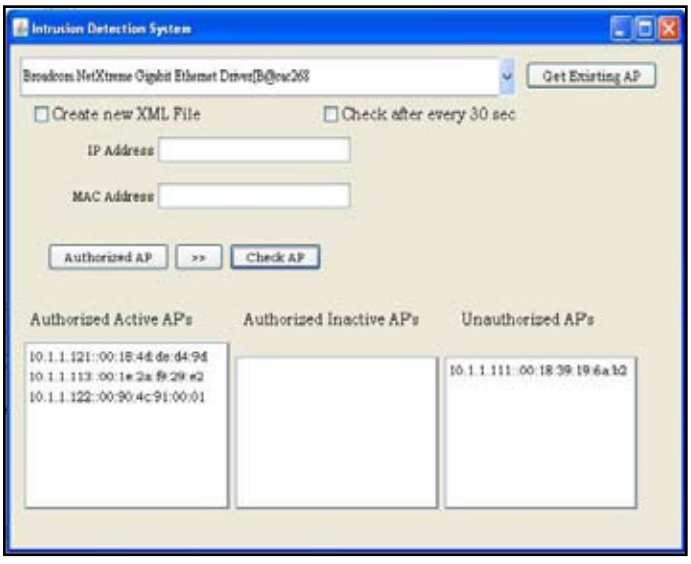


Fig. 3:

2. In this two authorized Access Points are being switched off and then clicked on Check AP button. Then it will get the existing Access Points information like IP address and MAC address on the network and check with the authorized Access Points IP address and MAC address information stored in XML file if any IP address is not in the XML file then it will consider it as rogue Access Point and if any IP address is in XML file which is not received while checking then it will consider it as inactive Access Point and display it in Authorized Inactive AP window (fig. 4).

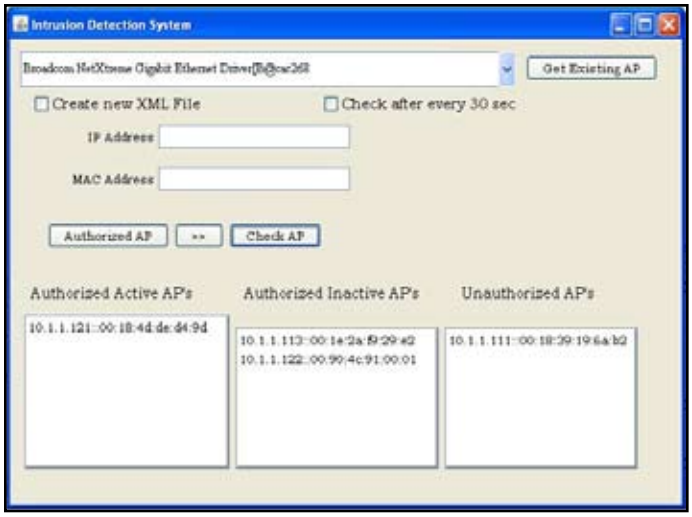


Fig. 4:

3. Then one of the Access Point is switched on which is switched off and following is the result (Fig 5).

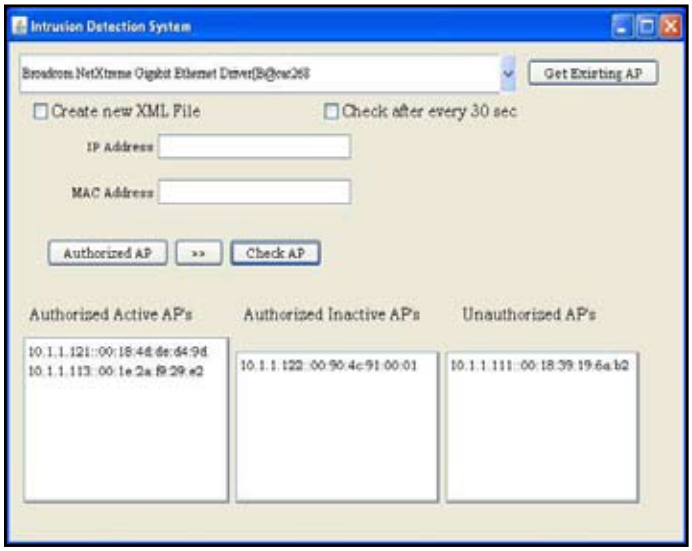


Fig 5

H. Blocking Mechanism

It is important to block Evil Twin Access Points detected on network to prevent leakage of confidential information and to reduce the probability of network attacks launched by attackers using Evil Twin Access Points. To achieve this, we used smurf attack technique to launch denial-of-service attack Evil Twin Access Points detected by our solution. In particular, when Evil Twin Access Points are detected by our approach we send a large number of ICMP packets with the spoofed IP address of Evil Twin Access Point and broadcast them on a network using IP broadcast address. For example on 10.0.0.0 network IP broadcast address is 10.255.255.255. The effect of this is all computers on network replay to the ICMP packets that causes a significant amount of traffic to the Evil Twin Access Point. Thus, it effectively causes a denial-of-service attack on Evil Twin Access Points. We continue sending spoofed ICMP packets on the network until the Evil Twin Access Points stops responding.

To block Evil Twin access points we send minimum size of ICMP packets using spoofed IP address of Evil Twin access points. The

minimum size of spoofed ICMP packets is 64 bytes. If the number of Evil Twin access points detected on the network are "n" then we send "n" number of spoofed ICMP packets, hence the total number of bytes we send are 64 × n. We argue that modern networks have gigabits of capacity, hence the network overhead introduce by our approach is very minimum. The packet overhead introduced on the network by our solution is affordable when compared to reliability provided by our approach in detecting and preventing Evil Twin access points.

I. Effectiveness

To measure the effectiveness of our approach, we injected an Evil Access Points in our wireless network. We ran our software on central server, which periodically sent fake ICMP broadcast packets and captured reply from Access Point devices. We checked IP address and MAC address of devices from captured reply packets and verified them with our authorized AP Point database. Our approach successfully detected the Evil Access Point on our test scenario.

V. Limitation and Future Work

Our current approach detects Evil Access Points using fake broadcast packets. In case of network partitioning our approach will not be able to detect Evil Access Points. For example, if an organization's internal network address is 192.168.1.0 and attacker configured Access Points to use 192.168.2.0 network. In such scenario, both networks are different and our current implementation aims to detect Evil Access Points on organization's network. Hence with our current implementation we will not be able to detect Evil Access Point on another network. However, we argue that if attacker's Evil Access Point is not connected to the organization network then he will not be able to Access organization's network resources. Only victim organization's employee computers who are configured to connect to DHCP server will connect to Evil Access Points and vulnerable to various attack vectors from attacker.

VI. Conclusion

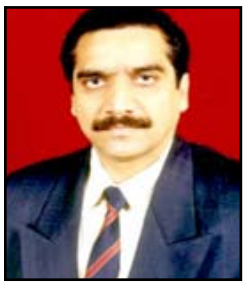
In this paper, we have presented the simple Intrusion Detection and Prevention Approach for Evil Twin Access Points in Wireless LAN. This technique will work on any type of network that is wired network, wireless network or heterogeneous network but only the constraint is all the nodes must be in the same subnet. This solution will not increase the traffic of the network as well as the server machine is sending only one fake broadcast packet on the network and reply will be send only by Access Points on the network where as rest all the devices which received this packet are going to discard the packet.

References

[1] Hao Han, Bo Sheng, Chiu C. Tan, Qun Li, Sanglu Lu, "A Timing-Based Scheme for Rogue AP Detection", 2011.
[2] Taebeom Kim,Haemin Park, Hyunchul Jung, Heejo Lee,"Online Detection of Fake Access Points using Received Signal Strengths", 2012
[3] Qu, G., Nefey M.M.,"RAPid.An indirect Rogue Access point Detection System", IEEE 2010.
[4] Roth, V., Polak, W., Rieffel, E. Turner, T.,"Simple and effective defense against Evil Twin Access Points", WiSec'08, March 31–April 2, 2008, Virginia,USA, 2008.
[5] Chao Yang, Yimin Song, Guofei Gu,"Active User-side Evil Twin Access Point Detection Using Statistical Techniques", 2011.
[6] Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou,"A Novel Approach for Rogue Access Point Detection on the Client-Side", 2012.
[7] Raheem Beyah Georgia Tech, Aravind Venkataraman Cigital,"Rogue-Access-Point Detection, Challenges, Solutions, and Future Directions", 2011.
[8] [Online] Available: http://www.blog.kaspersky.com/do-you-use-free-wifi-hotspots-a-survey.
[9] public wi-fi useage survey, Identity Theft Resource Center, 2012.

Sachin Rohidas Sonawane,Student of M.Tech Computer, BVDUCOE, Pune Maharashtra, India

Sandeep Vanjale Ph.D Student, BVDUCOE, Pune, Maharashtra, India



Dr. P.B.Mane, Professor, AISSMS IOIT, Pune, Maharashtra, India