Wifi Infrastructure Security System from Vulnerable Attacks

Thangaraj.P[1], Geethanjali.N[2], Kathiresan.K[3] and Madhumathi.R[4]
Department of computer science and engineering
Angel College of Engineering and Technology
Under Anna university, Chennai
Phone number : 9944072250

Abstract
Wi-Fi is a very popular wireless technology which is powerful core for the global digital infrastructure. A device connected using Wi-Fi can access the network resource such as the Internet via a wireless network access point. Recent discoveries and initiatives highlight a simple fact that the core is just as vulnerable as the edge. Wi-Fi can be less secure than wired connections because an intruder does not need a physical connection. Though security threats are imminent due to the open nature of communication, there are certain ways to protect the infrastructure of a network.In this paper, we examine the vulnerabilities of Wi-Fi network and this includes the intrusion detection in the security architecture of that network. We have shown such mechanism to solve arrival of intruders by Man-in –the-middle attack on a Wi-Fi network. Also, provide the steps to eliminate hackers from the Wi-Fi network and descriptions regarding the operations performed by different tools to avoid attackers from network. There are several holes in the wireless environment through which the attacks enter the network. In future those holes may be blocked completely by eliminating hackers from all attacks through which they enter. We also discuss a number of available solutions for controlling those threats.

Keywords
Wireless network, Wi-Fi infrastructure, Security threats, Vulnerability in Wi-Fi and MITM.

1 INTRODUCTION

The present world is in the need of compatible and portable products in all environments. As in our case the wired network system was left incompatible and towards the wireless environment by present users .while advantages over the wireless environment increases the vulnerabilities also increases. All computer users, from the most casual Internet surfers to large enterprises, could be affected by network security breaches. However, security breaches can often be easily prevented. This paper provides a general overview of the most common network security threats and the steps to protect the network from threats and ensure that the data traveling across the networks is safe. The attackers enter through the weak holes present in the wireless environment and make the disturbance to the environment and to the authorized users. We can prevent it by following some methodologies to avoid the attackers and restricting them.

1.1 Wireless environment

Wireless Networks have become ubiquitous in today's world. The interesting and compatible features of the wireless devices make the users to consume it for the communication. Millions of people use them worldwide every day at their homes, offices, and public hotspots to log on to the Internet and do both personal and professional work. People from government sectors and private sectors tend to use the wireless products for the communication. Though it offers the communication over the distance 120ft, the wireless communication is achieved through access point and ad-hoc hosts. Access point sends and receives the wireless signals to the client pc. Ad-hoc hosts are also act as the access points.

1.2 Wi-Fi technology:

Wi-Fi is the over the air network used by millions of computers across the world to connect up to each other and the internet. There are three terms which makes Wi-Fi working in portable devices.

1.2.1 Radio Signals: Radio Signals are the keys to make Wi-Fi environment. Wi-Fi antennas transmit these signals which are picked up by Wi-Fi receivers such as computers and cell phones that are equipped with Wi-Fi cards. When a computer receives any of these signals within the range of a Wi-Fi network, will read the signals and thus create an internet connection between the user and the network. Access points which consist of antennas and routers are the main source to transmit and receive radio waves.

1.2.2 Wi-Fi Cards: Wi-Fi card acts as an invisible cord that connects your computer to the Wi-Fi antenna for a direct connection to the internet. These cards can be external or internal. If Wi-Fi card is not installed in a computer, can attach a purchased USB antenna externally connect to your USB port or have an Wi-Fi antenna-equipped expansion card installed directly to that computer.

1.2.3 Wi-Fi Hotspots: A Wi-Fi hotspot can be created by installing an access point to an internet connection.

Manuscript received December 5, 2013
Manuscript revised December 20, 2013

Wireless signals are transmitted from the access point over a short distance of around 300 feet. Every Wi-Fi enabled devices can then connect to that network wirelessly. Few Hotspots require WEP key to connect to be private or secure. As it is an open connections, any device with a Wi-Fi card can gain access to that hotspot.

1.3 Wi-Fi standards:

The 802.11 standard is declared through several specifications of Wireless network. It defines an over-the-air interface between a wireless client and a base station or between two wireless clients.
There are several specifications in the 802.11 family:
802.11: This pertains to wireless LANs and provides 1- or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
802.11a: This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.
802.11b: The 802.11 high rate Wi-Fi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. Note that 802.11b was actually an amendment to the original 802.11 standard added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.
802.11g: This pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.

2 DESIGN AND SPECIFICATION

Wi-Fi network is introduced to make use of the most of scarce resources, are sometimes seen as unnecessary in the inexpensive WAPs, where wireless seems so economical. Survey should still perform to determine the optimal locations for WAPs to minimize channel interference while maximizing the range.

2.1 Setting a Wi-Fi Network:

Setting up a Wi-Fi network will allow the computers to get internet connection without plugging in an Ethernet cable. The user can also share any type of files from one computer to the other computers wirelessly and make it easy to stream music and video to any device on the network. Even some old PCs that don't have wireless card, there is an alternative that most Wi-Fi routers have a few Ethernet ports as well.

Before get start to build the network, builder must have a wireless router, some wireless network interface cards, if it is built in then don't for that user's computers.
Once user has a router the next step is to choose a good location. Install router in a central location so that every room in that place is covered by the Wi-Fi signal.
Here are 5 Steps to connect a Wi-Fi network in a domain

i) Ready the Wi-Fi enabled devices.
ii) Turning it on
iii) Set up the network
iv) Turn on encryption
v) Connect and access the network

Person who identify a best technique to access the confidential information in any network are hackers. It does not mean that the internet is not the safest media to share the information from hackers. Though intruders intrude the network it is impossible to attain the process completely. Safety measure in the place is very important that to minimize the risk of identified theft in a corporate network. Recent crime in online media is increase of registered intrusion activities in corporate network which is a serious issue in both government private organizations and also the individuals who are connected together in a network.

2.2 Detection of intruders:

Person who identify a best technique to access the confidential information in any network are hackers. It does not mean that the inter net is not the safest media to share the information from hackers. Though intruders intrude the network it is impossible to attain the process completely. Safety measure in the place is very important that to minimize the risk of identified theft in a corporate network. Recent crime in online media is increase of registered intrusion activities in corporate network which is a serious issue in both government private organizations and also the individuals who are connected together in a network.

2.3 Restriction from future attacks:

Hackers are mischievous to the network holders; they find a particular network and perform attack on that network without printing their footprints. Those attacks may be more dangerous to the network, due to lack in identifying the intruders who attacks the network. Provides more security features to the authenticated users of that particular user and also provide the alternative technique to avoid the attack by which the intruders enter the network. The intruders are identified by their IP and MAC address they used.

3 RELATED WORKS

3.1 Wi-Fi threats:

In Wi-Fi there is high possibility of threats, where it is the main source of danger. 802.11n products have matured to the point where many enterprises are investing huge for faster WLANs to support mission-critical applications. Here, we offer our Top Ten Wi-Fi Threats and explain why diligence is required.

- Data Interception
- Denial of Service
- Rogue Aps
- Wireless Intruders
- Misconfigured Aps
- Ad Hocs and Soft Aps
- Misbehaving Clients
- Endpoint Attacks
- Evil Twin Aps
- Wireless Phishing

Hackers perform attacks to threaten the users in the network. The threats are only the fact of danger that will be induced the components or the users through sensible attacks.

3.2 Wireless Security Attacks and Vulnerabilities:

3.2.1 Encryption-Based Attacks

To make secure the wireless network the encryption of data is used. Based on the 802.11 protocol, first encryption technique Wired Equivalent Privacy (WEP) was introduced. It marks protecting the integrity of data being sent over the network. Later WEP was superseded by Wi-Fi Protected Access (WPA) which was developed by the Wi-Fi Alliance to temporary replace the WEP standard as a more secure alternative. WPA features were intended to protect the network from WEP attacks.

3.2.2 WEP Attacks

This algorithm is mainly concentrate on the IEEE 802.11 wireless network. It is widely in use and is often the first security choice presented to users by router configuration tools.

Shamir who published an article describing the weakness in 2001.The FMS attack takes advantage of correlations between the WEP IVs and the key stream produced by the RC4 cipher to break the WEP key byte by byte.

3.2.2.1 FMS Attack

The first attack on the WEP protocol was called the FMS attack which was named after Fluhrer, Martin, and

3.2.2.2 Korek Attack

Another famous attack was developed by an internet user posting under the name of KoreK. KoreK released a cracking suite on an internet forum which implemented 17 different attacks. While some of these attacks were previously discovered, most were found by KoreK. The first group is similar to the FMS attack using the first word of output from the RC4 algorithm to recover the key.

3.2.2.3 PTW Attack

The newest and most powerful attack on WEP is called the PTW attack which is named after its creators Pyshkin, Tews, and Weinmann and released in 2012. The PTW is much more powerful than all the other attacks because it can make use of every packet captured.

3.2.3 WPA Attacks

3.2.3.1 Chop-Chop Attack

The TKIP is countered by the Chopchop attack and not by key recovery attack. Attacker decrypts the last m bytes of plaintext of an encrypted packet by sending m*128 packets to the network in average. It relies on the weakness of the CRC32 checksum called the ICV which is appended to the data of the packet. If this attack is successes then attacker can decrypt a WEP data packet without knowing the key. This can even work against dynamic WEP. This not recovers the WEP key itself, but reveals the plaintext. Some access points are not vulnerable to the attack. Some may seem vulnerable at first but they drop data packets shorter than 60 bytes. If access point drops packets shorter than 42 bytes, then tries to guess the rest of the missing data, where the headers are predictable. If an IP packet is captured, it checks that the checksum of the header is correct after guessing the missing parts of it. This requires at least one WEP data packet.

3.2.4 WPA2 Attacks

WPA2 is introduced with a new interoperability testing certification from the Wi-Fi Alliance. It is most secure form of encryption used on wireless networks with Robust Security Network (RSN) mechanism supports all of the mechanisms available in WPA. It contains advanced features of all other protocols.

The resultant features are explained in the below graph note in Firure1

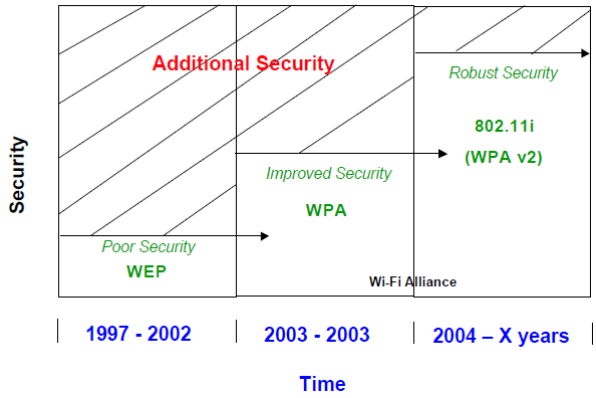

Figure1: Security graph

3.3 Other attack:

3.3.1 Man In The Middle Attacks

A man-in-the-middle attack can succeed only when the attacker can impersonate each side endpoint to the satisfaction of the other users. This is the attack on mutual authentication. Majority of cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. SSL can authenticate one or both parties using a mutually trusted certification authority.This attack intercepts a communication between two wireless devices. In http transaction the target is the TCP connection is between client and server. The attacker splits connection into 2 links, one between the client-the attacker and the other between the attackers- the server, as shown in figure2. Once TCP connection is intercepted, the attacker acts as a proxy which is able to read, insert and modify the data in the communication.

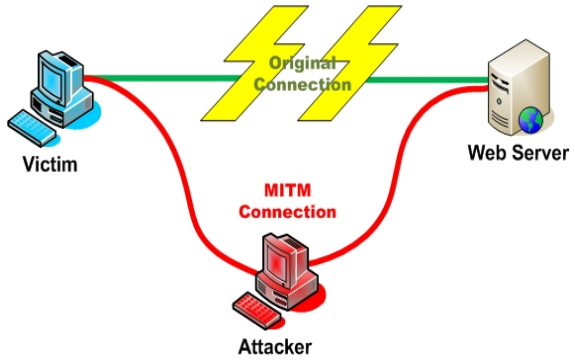

Figure2: Man-in-the-middle attack

3.3.2 ARP Poisoning Attacks

Address Resolution Protocol (ARP) poisoning is most common attack that is used to set up a Man in the Middle attack in other network. It is accomplished in two ways, spoofing ARP replies and sending spoofed IP packets. ARP is used to find the MAC address of the host with a specified IP address. If ARP table entry for the default gateway on the client is received by an attacker, then all packets the client tries to send out of the network which will first reach the attacker. A man in the middle attack along the lines of SSL strip can now be carried out. In order to access the network the network key has been cracked by this method.

3.3.3 The Hole 196 Attack

These attackers found "Hole196" vulnerability in WPA2 security protocol exposing WPA2-secured Wi-Fi networks to insider attacks of IEEE 802.11. Airtight Networks uncovers the weakness in WPA2 protocol, which has been documented.

Table 1: Risk table

RISK SHEET	
PROTOCOL	**MITM RISKS**
EAP-MD5	On public Ethernets or wireless LANs, station identities and password hashes can be easily sniffed. EAP-MD5 does not provide mutual authentication or EAP server authentication. Thus, MITM attackers may disguise as access points to deceive legal users into authenticating to the rouge AP.
EAP-TTLS	The systems protected by EAP-TTLS are still vulnerable to MITM attacks because user passwords can be more easily guessed, shared, or disclosed via social engineering than client-side certificates.
LEAP	The systems protected by LEAP are still vulnerable to MITM attacks.
PEAP	The systems protected by PEAP are still vulnerable to MITM attacks.
Key Fobs and One Time Password (OTP) tokens	Token-based and smart-card-based OTP systems are vulnerable to MITM attacks. Attackers may hijack online sessions by deceiving legal users into providing one-time-PINs produced by tokens or smart cards. Risk Level: MEDIUM
SSL	Credentials can sometimes be stolen in a MITM attack using a proxy server. Risk Level: LOW

4 IMPLEMENTATION

4.1 Attack implementation

Implementation of man in the middle attack involves the following attacking mechanisms which let the victim to fall in the attackers net.

4.1.1 Learning about the wireless environment

Basically the attacker tend to know about the features and working of wireless environment .

After getting some essential information such as

- Access point working standard
- Manufacture info
- Signal strength

• WPS protection status
• Security status
• Encryption status
• IP address range
• Packet filtering status

That information collected from the environment will help the attacker to implement the attack with preferred tools and techniques .Then the attacker tries to hack the encryption key.

4.1.2 Password recovery Attack

There are possibilities of recovering the WPA key in case of weak nature of password. (figure3)

Step1: attacker should capture the packets enough to find the password.

Step2: continue the capturing till getting valid handshakes

Step3: run the recovery tool aircrack-ng

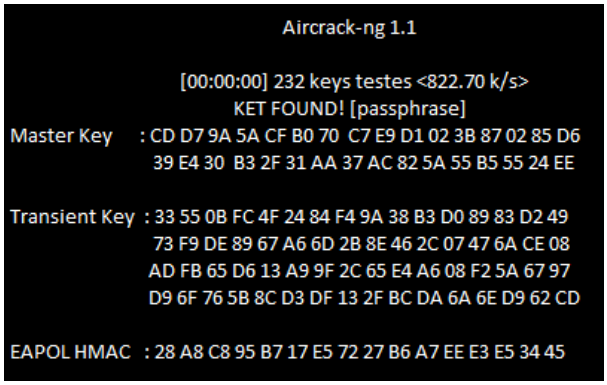

Figure 3: Password recovery attack using Aircrack-ng

4.1.3 Entering into WLAN – Replacing idle IP

Step1: scanning the IP status in the wireless network.

Step2: if idle IP found, attacker is lucky to implement further spoofing process.

4.1.4 ARP spoofing

Step1: to active the IP forwarding in the attackers' pc.

Step 2: perform ARP spoofing (Linux /windows) Linux is preferred. (figure 4).

4.1.5 Damaging the victim's process

Step1: altering the packets

Step2: victim gets damaged packets

4.2 Security implementation

Attackers enter the secured area through identifying its weakness.so authority should block the holes where the attacker enters.

4.2.1 Checking IP MAC address mapping

Step1: to monitor the ARP cache

Step2: periodically checking IP-mac mapping with arp cache identifies arp poisoning

Step3: identify the foot prints of attacker and restricting from future entry.

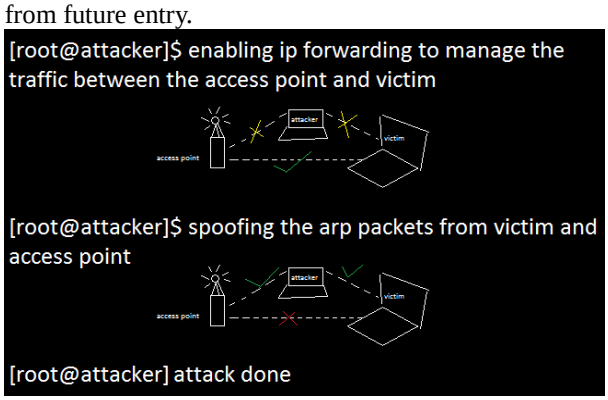

Figure 4: ARP spoofing using Backtrack 5

4.3 Wi-Fi security tools:

Tools are particularly efficient in LAN network environments, because they implement extra functionalities, like the ARP spoof capabilities that permit for communication between hosts.

Wi-Fi AP Discovery Tools
- Airodump-ng (Linux)
- NetStumbler (Win)

Wi-Fi Raw Packet Capture Tools
- Aircrack-ng Suite
- Ettercap

Wi-Fi Traffic Analyzers
- TamoSoft CommView for Wi-Fi
- WireShark (formerly Ethereal)

Wi-Fi Vulnerability Scanners and Assessment Toolkits
- Airbase
- BackTrack Penetration Testing Distribution
- Nmap, Zenmap
- WiCrawl

5 CONCLUSIONS

One who connected to the network he/she think to protect only their information from hacker but the thing to stop the hackers hacking the network. We have proposed a system to protect the infrastructure of the network and this paper mainly concentrate on issues to identify the footprints of the attackers. The hacker will not leave any type of evidence to find him so there are the certain steps to identify those hackers. Setting a wireless network is easier but to protect the infrastructure of the created one is find to be little difficult from vulnerabilities of outsiders. The attackers enter through the weak holes present in the wireless environment and make the disturbance to the environment and to the authorized users. We can prevent it the network from

those attackers by applying few methodologies provide in this paper. We also used some tools to hack the Wi-Fi infrastructure so that we are able to find the hackers idea on attacking the network. This paper also provides the technique to restrict the hackers from future threatens.

In future, able solve the ARP weaknesses. We can provide the built in functionality to expose the response from the true source with certain protocols. Expanded protocol is not available to say that one has to wait for the request to send a response. Enhance security feature of man-in-the-middle (MITM) attack from the hackers. Authenticated users can have special encrypted key which is use to protect their information as well as the infrastructure from the hackers to that network.

References

[1] Frederick T. Sheldon, Oak Ridge National Laboratory, John Mark Weber, Seong-Moo Yoo, and W. David Pan, "Insecurity Of Wireless Network" University of Alabama in Huntsville, IEEE Security & Privacy, July/August 2012

[2] Jose Nazario, Arbor Networks, John Kristoff, "Internet Infrastructure Security" Team Cymru - Copublished by the IEEE Computer and Reliability Societies, July/August 2012.

[3] O'Reilly, "802.11 Wireless Networks: The Definitive Guide -2002" <e-book>.

[4] Jaemin Lee,Chaungoc Tu, Souhwan Jung, "Man-in-the-middle Attacks Detection Scheme on Smartphone using 3G network", Soongsil University Seoul, Korea, 2012.

[5] Kevin Hulin, Carsten Locke, Patrick Mealey, and Ashley Pham, "Analysis of Wireless Security Vulnerabilities, Attacks, and Methods of Protection ", The University of Texas at Dallas , July 2011.

[6] Thrinatha R Mutchukota, Saroj Kumar Panigrahy, and Sanjay Kumar Jena, " Man-in-the-Middle Attack and its Countermeasure in Bluetooth Secure Simple Pairing", National Institute of Technology Rourkela, 769 008, Odisha, India, 2011.

[7] Dennis D. Steinauer, "Network Security in a Wireless World", National Institute of Standards and Technology, 2011.

[8] Utpal Paul, Anand Kashyap, Ritesh Maheshwari, and Samir R. Das, "Passive Measurement of Interference in WiFi Networks with Application in Misbehavior Detection", IEEE transactions on mobile computing, vol. 12, no. 3, march 2013

[9] Da Zhang, Member, "Enabling Efficient WiFi-Based Vehicular Content Distribution", IEEE, and Chai Kiat Yeo, IEEE transactions on parallel and distributed systems, vol. 24, no. 3, march 2013

[10] Min-kyu Choi1,Rosslin John Robles, Chang-hwa Hong and Tai-hoon Kim, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", Hannam University, Daejeon, Korea, July 2008.

[11] Hyunuk Hwang, Gyeok Jung, Kiwook Sohn, Sangseo Park, "A Study on MITM(Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP", The Attached Institute of ETRI, 2008.

[12] Pritam Gajkumar Shah (PhD, UC Australia), "Securing Wireless Sensor Networks- Challenges and Future Scope", 2008

[13] Puneet kumar and Prof. J.K. Sharma ,"Capacity Enhancement of 5G wireless networks", (IJAEST) International Journal Of Advanced Engineering Sciences And Technologies Vol No. 10, Issue No. 2, 228 - 233, 2010.

[14] Prasant Mohapatra, Chair, "Capacity Enhancement and Reliability of Wireless Mesh Networks", Office of graduate studies of the university of california davis, 2010.

[15] Yantao Li, Student Member, IEEE, Xin Qi, Matthew Keally, Zhen Ren, Gang Zhou, Member, IEEE, Di Xiao, Member, IEEE, and Shaojiang Deng, Member, IEEE, "Communication Energy Modeling and Optimization through Joint Packet Size Analysis of BSN and WiFi Networks", IEEE Transactions On Parallel And Distributed Systems, 2012.

[16] Loukas Lazos and Marwan Krunz, University of Arizona, "Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks", IEEE Network , January/February 2011.