Wireless Fidelity (Wi-Fi) - Threats and Security

Satish Kikani*, Harin Naik**

*(Developer - Tata Consultancy Services, B Wing Kensington Building IT/Tes/Sez, Hiranandani Business Park, Powai, Mumbai 400 076. Email: samkikani@gmail.com)
** (Editor - hackers5 Pvt. Ltd. 425, 4th Floor Gundecha Industrial Complex, Premises Co-op Society Ltd. Akurli Road, Grovel Bus stop, Kandivali (E), Mumbai 400 101. Web: http://hackers5.com Email: harry17in@gmail.com)

ABSTRACT

This paper explains about various threats to wireless networks, How hackers makes most use of it and what are the security steps one should take to avoid becoming victim of such attacks. Various threats explained here include Sniffing, Spoofing, DOS and Dummy LAN. Further this paper also explains various common ways to detect and prevent Hackers from stealing one's private valuable information.

Keywords – **WAP , Wi – Fi Security, WLAN Intrusion, Wireless Intrusion Detection System**

I. INTRODUCTION

Wi-Fi is very popular technology as it allows various electronics devices to exchange data wirelessly over computer network or internet connection. This networks are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards" and known as WLAN (Wireless Local Area Network). WLAN technology has become very popular in past few years due exponential growth in wireless technology. This technology has also grabbed attention of many hackers due to less security and ease of access. Various attacks which hacker performs are known as Sniffing, Spoofing, DDOS and Dummy/Rouge WLAN. Recently hackers were successful to hack into pacemaker by which hacker can control heart rhythms of a patient. There are various ways to prevent such attacks such as Proper configuration, secure protocols and wireless intrusion detection system.

II. THREATS OVER WLAN

1. Denial of Service (DoS)

A denial of service (DoS) occurs when a system is not providing services to authorized clients because of resource exhaustion by unauthorized clients. In wireless networks, DoS attacks are difficult to prevent, difficult to stop an on-going attack and the victim and its clients may not even detect the attacks. The duration of such DoS may range from milliseconds to hours. A DoS attack against an individual station enables session hijacking. Microwave ovens, baby

monitors, and cordless phones operate on the same unregulated radio frequency. Hacker can take advantage of this to generate large amount of noise in same frequency.
Due to this wireless LAN ceases to function.

The standard 802.11 encryption method, Wired Equivalent Privacy (WEP) is weak. As documented in the paper "Weaknesses in the Key Scheduling Algorithm of RC-4" [1]. After cracking WEP hacker authenticates many non-existing stations which look legitimate but there are nothing but randomly generated MAC addresses. Then he can send a flood of spoofed associate requests so that the association table overflows and network goes down.

2. Wireless Network Sniffing

Sniffing is eavesdropping on the network. A (packet) *sniffer* is a program that intercepts and decodes network traffic broadcast through a medium. Wire-Shark is very well known sniffer software.

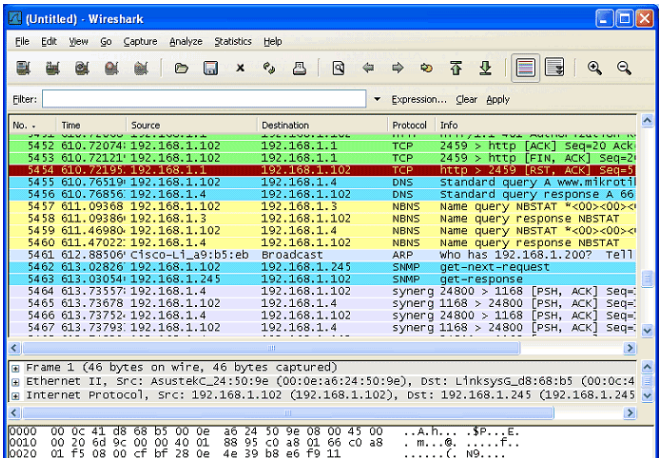

Fig.1 WireShark sniffing tool

Sniffing wireless network is very easy and safe as compared to wired LAN. Hacker can be far away or can be moving while he/she captures the data. Hacker can scan various channels without transmitting any data. Earlier various browsers and messengers used to transmit data as plain text and due to this hacker could easily access this information while staying anonymous.

3. MAC Address Spoofing

WAP (Wireless access point) controls the traffic and connection on network. It uses MAC address and IP address to identify the machines which can access the network. To stay hidden hackers uses MAC and IP address or victims machine.

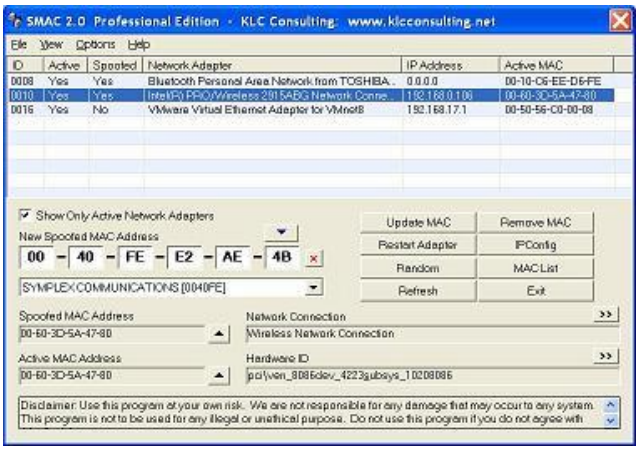

Fig.2 MAC Address spoofing tool

By using valid MAC and IP address, hacker can compromise WLAN easily. Hackers using various spoofing tools to change MAC and IP address programmatically.

4. Dummy/rogue WAP

Hackers can also attack and acquire sensitive information on WLAN introducing rogue WAP in to network. This can be configured to look like legitimate WAP. Since most of the wireless users connect to the WAP with best signal strength, users gets tricked in to using this dummy WAP. Once user connects to this WAP, hacker can access all the traffic through victims' computer.

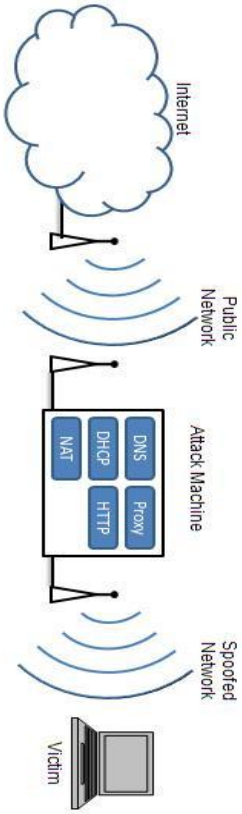

Fig.3 Dummy WAP Architecture

By creating this dummy WAP, hackers create back-door in the network. Such dummy WAP can be created very easily as devices used in such attacks are cheap and easily available. By creating such dummy WAP hacker can target many users at the same time. Due to this reasons this type of attack is most preferred by hackers and it is most dangerous also.

III. WIRELESS SECURITY BEST PRACTICES

1. Proper Configuration of WAP

Usually people use their wireless devices with default configuration which creates easy way for hackers. Default configuration of well-known manufacturers is easily available on the internet.

Manufacturer	Model	Version	Access Type	Username	Password	Notes
Cabletron	Netgear modem/router and SSR			netman	(none)	
NetGear	RM356	None	Telnet	(none)	1234	shutdown the router via internet
Netgear	MR-314	3.26	HTTP	admin	1234	
Netgear	RT314		HTTP	admin	admin	
Netgear	RP614		HTTP	admin	password	
Netgear	RP114	3.26	Telnet	(none)	1234	telnet 192.168.0.1
Netgear	WG602	Firmware Version 1.04.0	HTTP	super	5777364	
Netgear	WG602	Firmware Version 1.7.14	HTTP	superman	21241036	
Netgear	WG602	Firmware Version 1.5.67	HTTP	super	5777364	
Netgear	MR814		HTTP	admin	password	

Fig.4 Default Configuration List for NetGear Wireless Routers

In above figure we can see the default configuration of routers made by NetGear Company. These routers are most widely used in wireless networks. Following settings should always been changed from default one to prevent hackers from exploiting the devices.

1.1 Encryption settings.

1.2 SSID broadcast setting

1.3 Default Password

1.4 Use HTTPS instead of HTTP

1.5 Session Logging

2. Use of Secure Protocols

As mentioned above, WEP protocol with 802.11 standards are easy to crack. Net banking and online shopping is very common now. If hacker manages to crack the default encryption then he/she can easily get hold of sensitive user information such as Net Banking details, Passwords, Credit Card details etc.. To avoid this it is always advised to use secure protocol and encryption for wireless communication.

3. Wireless Intrusion Detection System (WIDS)

Wireless Intrusion Detection System (WIDS) is a computer system with specific hardware and software configuration. This system is used by security consultants to detect any behavior on the network which has same footprint as of attack by hackers. WIDS can also detect spoofed MAC address and session hijacking by hackers. It collects and analyzes the data from various devices on the network. WIDS also generates alerts on the basis on known attack patters. It can also detect dummy WAP.

4. Individual awareness

To avoid becoming victim of Wireless attack one should always be careful while using wireless networks. Following are some general best practices user should follow.

4.1 Configure firewall settings to treat WAP as public network.

4.2 Update Anti-Virus/ Operating System/ Firewall software.

4.3 Disable auto connect to Wi-Fi network settings.

4.4 Disable Wi-Fi when not using it.

4.5 Avoid using Net Banking or Shopping while using public Wi-Fi network.

4.6 If possible, avoid using public Wi-Fi network to access any service which require your login credentials

IV. CONCLUSION

Wi-Fi gives freedom to users so they can access network easily but at the same time it gives easy way to the hackers to penetrate and exploit the network if proper security is not there. Hackers can stay anonymous on wireless network with less effort and can easily target their victims by using various methods such as sniffing, dummy WAP etc.. In order to prevent such intrusion and detect such attacks we should always follow best practices such as changing default configuration, using Wireless intrusion detection systems and so on. If proper security is followed then security professionals can not only stop hackers from exploiting the network but also catch them by hacking the hacker.

REFERENCES

[1] "Wireless Intrusion Detection Systems" by Jamil Farshchi

[2] "HOW SECURE IS YOUR WIRELESS NETWORK?" By Tony Bradley (CISSP, MCSE2k, MCSA, A+)

[3] "Cisco Wireless LAN Security" By Tony Bradley (CISSP, MCSE2k, MCSA, A+)

[4] HANDBOOK OF INFORMATION SECURITY, VOLUME 3 edited by Hossein Bidgoli

[5] Default router configuration at "http://urbanwireless.info/"

[6] Wi – Fi Security tips at "http://www.fbi.gov"

[7] Wireless LAN Security Practices from "http://wirelessdefence.org"