

Wireless security: latest issues and security measures

Gurpinder Kaur, lecturer in SUSCET, Tangori

Abstract: This paper is based in wireless fidelity that is “Wi-Fi” an 802.11 IEEE standard.

The main issue in wi-fi system is the security issues in this paper the various security hazards are discussed a measures to overcome are also explained. here can be various mechanisms the are used for the wireless security e.g. MAC address filtering will prevent casual users from connecting to your network by maintaining a list of MAC addresses that are allowed access, (or not) but a serious cracker will simply scan your network traffic to find a MAC address that is allowed access, then change their equipment to use that address. Any new equipment will require another MAC address to be added to the list before it can be connected. Again, enabling MAC address filtering will not prevent anyone from reading the data that is transmitted without encryption. so various methods are explained in this paper.

I. INTRODUCTION:

Wi-Fi is short for "Wireless Fidelity," and it is the popular name for 802.11-based technologies. Ten to twenty years ago, everyone used modems to dial into a server (wow, remember when you first got a 2400-baud modem and thought you were fast. Compared to the early birds with their 300-baud modems, you were). Then, in the late 80's, early 90's, Ethernet started showing up in offices – these are the wires that look like phone cords except the wires are a little thicker and the plugs are a little bigger. They are also much faster – phone modems are pretty much limited to 56000 bits per second while the initial Ethernet was 10 million, 100 million is common today and 1000million equipment is available.

In fairly recent time (ca. 1999), the wireless protocols were proposed and in the last couple of years WiFi has become very common in offices and homes as a way to tie multiple computers together (i.e. network them) without needing to run wires to each computer. They are a little slower than Ethernet, but still much faster than phone connections. Concurrently with people setting these up in their homes and offices, some companies have started putting commercially available 'hotspots' - locations in airports, hotels and coffee shops (T-mobile® at Starbucks, for example) where you can receive and send signals so you can get connected on the road (of course, many of these places charge you for the privilege of using their connection).

In technical terms, WiFi has certain similarities to cordless phones (not wireless that you can use virtually anywhere, but cordless/portable that have a base station which plugs into .

your wall socket and a handset that you can use around your home). In fact, WiFi and cordless phones even use some of the same radio frequencies. Unlike cordless phones that have a matched pair of handset/base station, WiFi has much more flexibility. The 'base station' (called an access point or AP) can connect to multiple 'handsets' (WiFi equipped computers) or you can just connect computers to each other.

II. TYPES OF UNAUTHORIZED ACCESS TO COMPANY NETWORKS

A. Accidental association

Unauthorized access to company wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighboring company's overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network

B. Malicious association

“Malicious associations” are when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP). These types of laptops are known as “soft APs” and are created when a cracker runs some software that makes his/her wireless network card look like a legitimate access point. Once the cracker has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans. Since wireless networks operate at the Layer-2 level, Layer-3 protections such as network authentication and virtual private networks (VPNs) offer no barrier. Wireless 802.1x authentications do help with protection but are still vulnerable to cracking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the cracker is just trying to take over the client at the Layer-2 level.

C. Ad-hoc networks:

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

D. Non-traditional networks:

Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These non-traditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.

E. Identity theft (MAC spoofing):

Identity theft (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to only allow authorized computers with specific MAC IDs to gain access and utilize the network. However, a number of programs exist that have network “sniffing” capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.

F. Man-in-the-middle attacks

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a “de-authentication attack”. This attack forces AP-connected computers to drop their connections and reconnect with the cracker’s soft AP. Man-in-the-middle attacks are enhanced by software such as LANjack and AirJack, which automate multiple steps of the process. What once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

G. Denial of service

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection

messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

H. Network injection

In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcast network traffic such as “Spanning Tree” (802.1D), OSPF, RIP, and HSRP. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

I. Counteracting risks

Risks from crackers are sure to remain with us for any foreseeable future. The challenge for IT personnel will be to keep one step ahead of crackers. Members of the IT field need to keep learning about the types of attacks and what counter measures are available.

J. Methods of counteracting security risks

There are many technologies available to counteract wireless network intrusion, but currently no method is absolutely secure. The best strategy may be to combine a number of security measures.

IV. STEPS FOR WIRELESS SECURITY:

- A. All wireless LAN devices need to be secured
- B. All users of the wireless network need to be educated in wireless network security
- C. All wireless networks need to be actively monitored for weaknesses and breaches

V. METHODS TO SECURE WIRELESS NETWORKS:

A. MAC ID filtering:

Most wireless access points contain some type of MAC ID filtering that allows the administrator to only permit access to computers that have wireless functionalities that contain certain MAC IDs. This can be helpful; however, it must be remembered that MAC IDs over a network can be faked. Cracking utilities such as SMAC are widely available, and

some computer hardware also gives the option in the BIOS to select any desired MAC ID for its built in network capability.

B. *Static IP Addressing:*

Disabling at least the IP Address assignment function of the network's DHCP server, with the IP addresses of the various network devices then set by hand, will also make it more difficult for a casual or unsophisticated intruder to log onto the network. This is especially effective if the subnet size is also reduced from a standard default setting to what is absolutely necessary and if permitted but unused IP addresses are blocked by the access point's firewall. In this case, where no unused IP addresses are available, a new user can log on without detection using TCP/IP only if he or she stages a successful Man in the Middle Attack using appropriate software

C. *WEP encryption:*

WEP stands for Wired Equivalency Privacy. This encryption standard was the original encryption standard for wireless. As its name implies, this standard was intended to make wireless networks as secure as wired networks. Unfortunately, this never happened as flaws were quickly discovered and exploited. There are several Open Source utilities like aircrack-ng, weplab, WEPCrack or airtsnort that can be used by crackers to break in by examining packets and looking for patterns in the encryption. WEP comes in different key sizes. The common key lengths are currently 128- and 256-bit. The longer the better as it will increase the difficulty for crackers. However, this type of encryption has seen its day come and go. In 2005 a group from the FBI held a demonstration where they used publicly available tools to break a WEP encrypted network in three minutes. WEP protection is better than nothing, though generally not as secure as the more sophisticated WPA-PSK encryption. A big problem is that if a cracker can receive packets on a network, it is only a matter of time until the WEP encryption is cracked.

D. *WPA:*

Wi-Fi Protected Access (WPA) is an early version of the 802.11i security standard that was developed by the Wi-Fi Alliance to replace WEP. The TKIP encryption algorithm was developed for WPA to provide improvements to WEP that could be fielded as firmware upgrades to existing 802.11 devices. The WPA profile also provides optional support for the AES-CCMP algorithm that is the preferred algorithm in 802.11i and WPA2.

WPA Enterprise provides RADIUS based authentication using 802.1x. WPA Personal uses a pre-shared Shared Key (PSK) to

establish the security using an 8 to 63 character passphrase. The PSK may also be entered as a 64 character hexadecimal string. Weak PSK passphrases can be broken using off-line dictionary attacks by capturing the messages in the four-way exchange when the client reconnects after being deauthenticated. Wireless suites such as aircrack-ng can crack a weak passphrase in less than a minute. WPA Personal is secure when used with 'good' passphrases or a full 64-character hexadecimal key.

E. *WPA2:*

WPA2 is a WiFi Alliance branded version of the final 802.11i standard. The primary enhancement over WPA is the inclusion of the AES-CCMP algorithm as a mandatory feature. Both WPA and WPA2 support EAP authentication methods using RADIUS servers and preshared key (PSK) based security.

F. *LEAP*

This stands for the Lightweight Extensible Authentication Protocol. This protocol is based on 802.1X and helps minimize the original security flaws by using WEP and a sophisticated key management system. This also uses MAC address authentication. LEAP is not safe from crackers. THC-LeapCracker can be used to break Cisco's version of LEAP and be used against computers connected to an access point in the form of a dictionary attack.

G. *PEAP*

This stands for Protected Extensible Authentication Protocol. This protocol allows for a secure transport of data, passwords, and encryption keys without the need of a certificate server. This was developed by Cisco, Microsoft, and RSA Security.

H. *TKIP:*

This stands for Temporal Key Integrity Protocol and the acronym is pronounced as tee-kip. This is part of the IEEE 802.11i standard. TKIP implements per-packet key mixing with a re-keying system and also provides a message integrity check. These avoid the problems of WEP.

I. *RADIUS*

This stands for Remote Authentication Dial In User Service. This is an AAA (authentication, authorization and accounting) protocol used for remote network access. This service provides an excellent weapon against crackers. RADIUS was originally proprietary but was later published under ISOC

documents RFC 2138 and RFC 2139. The idea is to have an inside server act as a gatekeeper through the use of verifying identities through a username and password that is already pre-determined by the user. A RADIUS server can also be configured to enforce user policies and restrictions as well as recording accounting information such as time connected for billing purposes.

J. WAPI

This stands for WLAN Authentication and Privacy Infrastructure. This is a wireless security standard defined by the Chinese government.

K. Smart cards, USB tokens, and software tokens

This is a very high form of security. When combined with some server software, the hardware or software card or token will use its internal identity code combined with a user entered PIN to create a powerful algorithm that will very frequently generate a new encryption code. The server will be time synced to the card or token. This is a very secure way to conduct wireless transmissions. Companies in this area make USB tokens, software tokens, and smart cards. They even make hardware versions that double as an employee picture badge. Currently the safest security measures are the smart cards / USB tokens. However, these are expensive. The next safest methods are WPA2 or WPA with a RADIUS server. Any one of the three will provide a good base foundation for security. The third item on the list is to educate both employees and contractors on security risks

and personal preventive measures. It is also IT's task to keep the company workers' knowledge base up-to-date on any new dangers that they should be cautious about. If the employees are educated, there will be a much lower chance that anyone will accidentally cause a breach in security by not locking down their laptop or bring in a wide open home access point to extend their mobile range. Employees need to be made aware that company laptop security extends to outside of their site walls as well. This includes places such as coffee houses where workers can be at their most vulnerable. The last item on the list deals with 24/7 active defense measures to ensure that the company network is secure and compliant. This can take the form of regularly looking at access point, server, and firewall logs to try and detect any unusual activity. For instance, if any large files went through an access point in the early hours of the morning, a serious investigation into the incident would be called for. There are a number of software and hardware devices that can be used to supplement the usual logs and usual other safety measures

Steps in securing a wireless network:

L. Turn on encryption. WPA2 encryption should be used if possible. WPA encryption is the next best alternative, and WEP is better than nothing.

M. Change the default password needed to access a wireless device — Default passwords are set by the manufacturer and are known by crackers. By changing the password you can prevent crackers from accessing and changing your network settings

N. Change the default SSID, or network name — Crackers know the default names of the different brands of equipment, and use of a default name suggests that the network has not been secured. Change it to something that will make it easier for users to find the correct network. You may wish to use a name that will not be associated with the owner in order to avoid being specifically targeted.

O. Disable file and print sharing if it is not needed — this can limit a cracker's ability to steal data or commandeer resources in the event that they get past the encryption.

- a. Access points should be arranged to provide radio coverage only to the desired area if possible. Any wireless signal that spills outside of the desired area could provide an opportunity for a cracker to access the network without entering the premises. Directional antennas should be used, if possible, at the perimeter directing their broadcasting inward. Some access points allow the signal strength to be reduced in order to minimise such signal leakage.
- b. Divide the wired and wireless portions of the network into different segments, with a firewall in between. This can prevent a cracker from accessing a wired network by breaking into the wireless network.
- c. Implement an overlay Wireless intrusion prevention system to monitor the wireless spectrum 24x7 against active attacks and unauthorized devices such as Rogue Access Points. These systems can detect and stop the most subtle or brute force methods of wireless attacks, and provide you with deep visibility into the use and performance of the WLAN.

Here are some often-recommended security steps that are not usually of any benefit *against experienced crackers* (they will however prevent the larger group of inexperienced users from gaining access to your network easily, should they find your password). These are:

Disabling the SSID broadcast option — Theoretically, hiding the SSID will prevent unauthorized users from finding the network. In fact, while it will prevent opportunistic users from finding the network, any serious cracker can simply scan your other network traffic to find the SSID. It will also make it harder for legitimate users to connect to the network, since they must know the SSID in advance and type it in to their equipment. Hiding the SSID will not prevent anyone from

reading the data that is transmitted, only encryption will do that.

Enabling MAC address filtering — MAC address filtering will prevent casual users from connecting to your network by maintaining a list of MAC addresses that are allowed access, (or not) but a serious cracker will simply scan your network traffic to find a MAC address that is allowed access, then change their equipment to use that address. Any new equipment will require another MAC address to be added to the list before it can be connected. Again, enabling MAC address filtering will not prevent anyone from reading the data that is transmitted without encryption.

Mobile Devices and Wireless IPS:

With increasing number of mobile devices with 802.1x interfaces, security of such mobile devices becomes a concern. While open standards such as Kismet [external link] is targeted towards securing laptops, access points solutions should extend towards covering mobile devices also. Host based solutions for mobile handsets and pda's with 802.1x interface.

Security within mobile devices fall under 3 categories:

- a. Protecting against ad hoc networks
- b. Connecting to rogue access points
- c. Mutual authentication schemes such as wpa2 as described above

Countering Lack of Security in Wi-Fi Hot Spots

Public hotspots are not secure, not even turned on with Wired Equivalent Privacy (WEP), the 1999-era security standard of 802.11 Wi-Fi communications, making them a risk for any business professional to use, says Mike Disabato, senior analyst with the Burton Group.

In a report on "Securing the Mobile Device," Disabato outlines options that users tapping the 802.11 protocol have for securing their transmissions and guarding the integrity of their data.

At a minimum, the mobile user should be using an encrypted VPN over 802.11 to secure the transmission. In addition, the user should have a personal firewall, should be running a virus scan and spyware remover, and possibly should be encrypting sensitive files.

Newer vulnerabilities include connection sharing, set by defaults in the original Windows XP operating system by Microsoft, which can allow access to an enterprise network and/or the content of the communicating device, and the

wireless technology now built into many laptop PCs (either Bluetooth or 802.11).

Bluetooth is less of a risk than 802.11 because the range is not as great, the association mechanism is more strict, and it has good encryption features. The 802.11 security options include WEP, Wi-Fi Protected Access (WPA and WPA2) and 802.11i/AES, expected to be available later this year after IEEE committees ratify the standard.

Those users without strong protection, who are using 802.11 communications for business, need to be aware of the risks.

"Public hot spots are not secure and even if the user's machine is WEP-enabled, it takes about 30 minutes to crack WEP using tools easily available to hackers," Disabato says.

The encrypted VPN options include IPSec and SSL. IPSec provides full use of network resources, including legacy applications, and provides strong authentication via a unique client on each user device. It is limited by the requirements that client software must be installed and managed on the device, and that firewalls must be configured to accommodate it. It is well-suited for applications including site-to-site VPNs, telecommuter VPNs and voice and data traffic.

SSL VPNs provide a "clientless" extranet option and freedom to user any remote access device with a browser. The session is specific to an application or server to access control is tight. Its drawbacks include limited to Web applications over HTTP and slower performance due to SSL handshaking. It is well-suited for enterprise applications portals and e-business applications such as business to business or business to consumer.

"For most Web-based applications, SSL will be fine," Disabato says. "For power users who need legacy application access in particular, IPSec is a better option."

For security managers to get a handle on remote users, he suggests conducting "a risk assessment of all the information that will travel over the mobile connection. Use encrypted VPNs or remote authorization. And have the security system be the same for your people no matter what device they use or where they are."

CONCLUSION:

This paper concludes the latest steps taken to the security of wireless networks for the protection of the data from the unauthorised access

REFERENCES:

- A. Introduction to Wireless Network Security From Tony Bradley, CISSP-ISSAP, Your Guide to Internet / Network Security.
- B. http://netsecurity.about.com/od/hackertools/a/aa072004b_2.htm
- C. Maximum Wireless Security (by Cyrus Peikari (Author), Seth Fogie (Author)
- D. Wi-Foo: The Secrets of Wireless Hacking by Andrew Vladimir
- E. Wireless Communications Security (Artech House Universal Personal Communications) by Hideki Imai