State of Affairs of Wireless Networks

Rakesh Arora
GSEC Version 1.4b
30th Jan 2003

1. Abstract

Wireless Networks have become very common place in the recent past. Hotspots have come up in airports, coffee shops, hotels etc because the cost of setting up a wireless network has plummeted in the past few years. And add to it the convenience of having no wires snaking around the building. Wireless networks have gained so much popularity that there are millions of home networks set up and many of them are offering internet usage free for by-passers. However, companies are a little more skeptical than others to set up wireless networks in their offices. Their concern is justified because the security in wireless networks is not enough and a hacker can break their security with a little effort and free tools available from the Internet. In this paper, we talk about the fundamentals of wireless network, the built-in security (or in-security) that comes with those networks, some of the tools that can be used to audit the wireless network and finally discuss how to safeguard the network by deploying additional security.

2. IEEE Standards

The most common wireless networks that are out there today are based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11b technology. The base technology is IEEE 802.11, which supports data rates of 2 Mbps. In the recent years, several technologies derived from the 802.11 and these are 802.11a, 802.11b and 802.11g. The standards were developed so that one vendor's product (wireless cards or access points) that are Wi-Fi certified, will be compatible with any other vendor's Wi-Fi certified products.

2. 1 IEEE 802.11

The IEEE 802.11 standard was approved in 1997 and it defines the physical layer options for wireless transmission and MAC layer protocol. The standard defines protocols for two variants of the network: Adhoc networks and Infrastructure networks. An adhoc network is a simple network where communications are established between multiple stations in a given coverage area without the use of an access point or base station. All the nodes are assumed to be peers. The infrastructure mode uses an access point that controls the allocation of transmit time for all stations/clients and allows clients to roam from cell to cell. The access point is used to handle the traffic from the mobile radio to the wired or wireless backbone of the infrastructure network. [1][4]

IEEE 802.11 provides for two variations of the physical layer. They are two radio frequency (RF) technologies namely Direct Sequence Spread Spectrum (DSSS) and Frequency Hopped Spread Spectrum (FHSS). Both the DSSS and FHSS operate in the 2.4 GHz of the Industrial, Scientific and Medical (ISM) band. This was chosen because you don't need a license from the Federal Communications Committee (FCC) to operate on it. With DSSS, the transmission signal is spread over an allowed band and a random binary string is used to modulate the transmitted signal. This random signal is called the spreading code. The data bits are mapped to into a pattern of "chips" and mapped back into a bit at the destination. The number of chips that represent a bit is the spreading ratio. The higher the spreading ratio, the more the signal is resistant to interference. Recovery is faster in DSSS systems because of the ability to spread the signal over a wider band. DSSS systems provide a wireless network with both a 1 Mbps and 2 Mbps data payload communication capability. According to the FCC regulations, the DSSS system shall provide a processing gain of at least 10 dB. The DSSS system uses baseband modulations of Differential Binary Phase Shift Keying (DBPSK) and Differential Quadrature Phase Shift Keying (DQPSK) to provide the 1 Mbps and 2 Mbps data rate respectively.[5]

FHSS splits the band into many small subchannels (1 MHz). The signal then hops from subchannel to subchannel transmitting short bursts of data on each channel for a set period of time, called dwell time. The hopping sequence must be synchronized at the sender and the receiver or information is lost. The FCC requires that the band be split into at least 75 subchannels and that the dwell time is no more than 400 ms. Frequency hopping is less susceptible to interference because the frequency is constantly shifting. This makes frequency-hopping systems extremely difficult to intercept. In order to jam a frequency hopping system, the whole band must be jammed. These features are very attractive to agencies involved with law enforcement or the military.[7]

2.2 IEEE 802.11a

It uses the 5 GHz unlicensed ISM band and provides support for data, voice and images. Instead of using BPSK or QBPSK, this uses Orthogonal Frequency Division Multiplexing (OFDM). This proposal was set forth by NTT and Lucent Technologies, which the IETF standard body accepted. The OFDM system provides a wireless LAN with data payload communications capabilities of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. The support of transmitting and receiving data rates of 6, 12 and 24 Mbps is mandatory. The system uses 52 sub carriers that are modulated using binary or quadrature phase shift keying (BPSK/QPSK), 16-quadrature amplitude modulation (QAM) or 64-QAM.[2]

2.3 IEEE 802.11b

This standard also came out in 1999 and gained much more popularity than the 802.11a. It uses the 2.4 GHz band and can support data rates upto11 Mbps. The data rates that it supports are 1, 2, 5.5 and 11 Mbps. Complementary Code Keying (CCK) is used as the modulation scheme to provide the higher rates. CCK modulation was proposed by Harris and Lucent Technologies and allows a maximum throughput of 11 Mbps. The chipping rate is 11 MHz, which happens to be the same as that of the DSSS system, thus providing the same occupied channel bandwidth. CCK allows upto 8 bits to be packed in a symbol and the symbol rate is increased to 1.375 million symbols/sec. Thus speeds of 11 Mbps can be achieved using CCK. In addition to providing higher speed extensions to the DSSS system, a number of optional features allow the performance of the radio frequency LAN system to be improved as technology allows the implementation of these options to be cost effective. A key benefit of CCK is its resistance to multi-path interference. This allows CCK based devices to be less susceptible to multi-path interference thereby allowing the wireless LANs to provide system performance. In addition to the CCK modulation, another technique that is available is Packet Binary Convolutional Coding (HR/DSSS/PBCC). Another optional capability is Channel Agility. This option provides for IEEE 802.11 FH PHY interoperability with High Rate PHY of IEEE 802.11b.[3][6][11]

2.4 IEEE 802.11g

This is not a standard yet but the 802.11g task group is expecting to get the final approval by June/July 2003. It will support data rates of up to 54 Mbps, which is the same for 802.11a. However it will operate in the 2.4 GHz frequency range, thus making it compatible with the widely deployed 802.11b. Additional security has also been added to it. An 802.11g hardware will coexist with the 802.11b hardware. If you have an 802.11g access point, both 802.11g and 802.11b clients will be able to communicate with the access point. Likewise a 802.11b client will be able to access a 802.11b access point. The 802.11g draft standard has two mandatory modes. These are

a) CCK for backward compatibility with 802.11b, and
b) OFDM, offering 802.11a data rates in the 2.4 GHz frequency spectrum.

The optional modes that it can support are CCK-OFDM and PBCC-22 [8]. Since it is compatible with 802.11b devices, so a lot of vendors are working towards making access points having the 802.11b/802.11g combo.

3. Security Concerns

The default authentication protocol for IEEE 802.11 networks is Open System authentication. The other authentication protocol suggested by the IEEE standard is Shared Key authentication. Open System authentication provides a null authentication process, i.e., it authenticates any client who requests authentication. The shared key authentication is based on the challenge/response paradigm. Wired Equivalent Privacy (WEP) provides for the encryption of packets exchanged between the client and the access point. In this form of authentication, the client requests the access point that it be authenticated. In response, the access point sends the client a challenge text. The client then uses its shared key to encrypt the text and sends it back to the access point. Since the shared key is symmetric, so the access point can use the same key to decrypt the data received. If the data recovered on decrypting the packet is the same as the challenge text, then the client has been authenticated.[15]

3.1 Weakness of WEP

WEP, as the name implies, was meant to provide the same level of security as a wired network but it falls way short because of the vulnerabilities in its algorithm. There are free tools available that exploit those vulnerabilities, enabling even novice hackers to be able to break the WEP key and hence get a foot in the door of that wireless network.

We discuss the operation of WEP, so as to shed some light on its vulnerability. The sender generates a 24-bit Initialization Vector (IV) and appends this to the shared key (either 40-bit or 104-bit) to come up with a unique key for each packet. It then calculates the Cyclic Redundancy Checksum (CRC) of the data to be transmitted and appends it to the data. The 64-bit or 128-bit "unique" key is then sent through a RC4 Pseudo Random Number Generator (PRNG). The generated key stream (64-bit or 128-bit) is then XORed with the plaintext data and CRC to create the cipher text. After setting a bit in the header to indicate that it is WEP encrypted and inserting the IV into an appropriate field of the header, the frame with the cipher text is sent to the receiver.

The weakness of WEP arises from the usage of IV and the RC4 stream cipher. The IV is 24 bits long and after 2^{24} keys, the IV starts repeating. Now, since a stream cipher (RC4 in this case) can never be reused, it implies that the shared key needs to be changed to prevent hackers from determining the key. Since it is not practical that the shared key will be replaced as soon as 2^{24} packets have been transmitted (which could be in every couple of hours), so we end up having duplicate keys and hence are susceptible to attacks. There are tools like WEPcrack and Airsnort that are freely available, which make use of the weakness of WEP algorithm and determines the shared key after a few hours of collection of data. [14]

3.2 Other Shortcomings

The authentication between the client and access point is only one way – the access point authenticates the client but the IEEE 802.11 standard doesn't provide for authenticating an access point. This is a serious limitation and has been made use of by hackers. If you can set up an access point outside an office building so that the signal from it is strong enough within the building, then legitimate clients can mistakenly connect to your access point in the parking lot, instead of the authenticated access points. This will enable the parking lot hacker to have access to all the data that the client computers are transmitting, some of which could be corporate secrets. Another shortcoming is that the IEEE 802.11 doesn't standardize the key management. This allows vendors to come up with different implementations or maybe none at all.

4. Security proposed by 802.11i Task group

The 802.11i task group is responsible for enhancing the security and authentication mechanism for 802.11 MAC. The group is working on 802.1x, an IEEE standard that provides an authentication framework for 802 based LANs. 802.1x is not tied to any networking protocol but acts as a basis for defining a means of authenticating the clients. 802.1x provides user based authentication and centralized key management and distribution. The user authentication is provided by Extensible Authentication Protocol (EAP). [10]

There are three entities involved in a 802.1x network architecture. The first is a client seeking permission to the wireless network and is also known as the supplicant. The second is the access point (also known as the authenticator in 802.1x standard). The last is the centralized authentication server (mostly RADIUS server). The supplicant seeks to use some service offered through a port on the authenticator. The permission request is forwarded to the authentication server and based on its response, the authenticator either grants or denies access to the port/service. 802.1x still suffers from the fact that it provides only one-way authentication. The client is authenticated to the access point but the client doesn't authenticate the access point. This loophole (lack of mutual authentication) can be used to perform man-in-the-middle attacks if the higher layer protocol also performs a one way authentication (eg., EAP-MD5).[13]

To provide a secure means of transporting authentication data, the task group is looking at two IETF drafts – Tunneled Transport Layer Security (TTLS) and Protected Extensible Authentication Protocol (PEAP). Both of them provide a secure transport medium by using a tunnel between the client and the authentication server. The standard will allow to set up an end-to-end tunnel without the need of having certificates.[17]

5. Interim solution

Several vendors have come up with a new standard called Wi-Fi Protected Access (WPA) to provide additional security for wireless networks. The birth of WPA resulted because of the need for better data encryption and user authentication. WPA is meant to be an interim solution and will try to fill the security void until the 802.11i draft is standardized. WPA proposes two security enhancements. The first is the usage of Temporal Key Integrity Protocol (TKIP) to provide better data encryption. TKIP provides better encryption by using a larger Initialization Vector, a message integrity check and a per packet key mixing function. It also provides for a better key management.

The second enhancement is the use of EAP to authenticate the users. It provides a two way authentication, so that it does not fall victim to man-in-the-middle attacks. WPA is a subset of the 802.11i and will be forward compatible with it. The additional security measures that 802.11i will provide are enhanced encryption protocols like AES, secure disassociation and de-authentication, secure IBSS and secure fast handoff. [16]

6. Tools Available

A lot of wireless tools (mostly free) useful for auditing the wireless network have come up in the past couple of years. Some of the common ones are:

NetStumbler (http://www.netstumbler.com) – this works on the windows platform and uses active scanning for networks. There is also a version for handhelds (having windows CE as the operating system) called MiniStumbler. It works on cards having the Hermes chipset.

Kismet (http://www.kismetwireless.net) – this is one of the most popular tool for the Linux platform. It is a passive sniffer and hence can't be detected by other tools. There is a version for the handhelds that have Linux as their operating system (e.g. zaurus from Sharp)

Wellenreiter (http://www.remote-exploit.org) – this works on Linux and BSD platforms. There is also a handheld version running on Linux. It is a gtkperl program that makes the discovery and auditing of 802.11b networks easier.

Ethereal (http://www.ethereal.com) – It is one of the most popular network analyzers for wired networks. But in the past few months, it has been able to understand 802.11b networks and it can detect wireless networks on linux and BSD. It is currently not able to detect wireless networks on windows, as there are currently no free drivers to put the card into monitor mode in windows.

MacStumbler (http://www.macstumbler.com) – this is a Macintosh version of NetStumbler. Like Netstumbler, it is also an active auditing tool (sends out probe requests and waits for probe responses). It currently only works with airport wireless cards.

Airsnort (http://airsnort.shmoo.com) – this is a wireless tool that is commonly used to break the WEP encryption. It passively listens for packets on a linux box, and when enough data has been collected for the network, it can break the encryption key. It capitalizes on the vulnerability of WEP, as has been documented in several papers.

Airopeek NX (http://www.wildpackets.com) – this is a commercial product offered by Wildpackets and sells for over $2000. This tool works on windows and unlike Netstumbler, it works with all of Hermes, Prism and Cisco chipsets. It is probably the best commercial wireless auditing tool. Some of the other commercial auditing tools are Sniffer Wireless from Network Associates (very expensive) and AirMagnet (comparable in pricing to Airopeek NX).

AirDefense IDS (http://www.airdefense.net) – this is more than just a wireless auditing tool or sniffer and it presumably the wireless industry's first Intrusion Detection System (IDS). It detects rogue wireless WLANs, intruders, attacks, vulnerabilities and attempts to protect the wireless by responding to attacks. It sends real time updates to a centralized console to alert the system administrator.

Currently, Netstumbler and Kismet have turned out to be the most popular wireless auditing tool for windows and linux platform, respectively. Numerous people carry their laptop or handheld running a wireless sniffer, with high gain antennas mounted on the roof of their car, to log wireless networks when they are driving past a residential or commercial neighborhood. This has become very popular and is commonly known as War Driving. A few war-driving efforts have been organized in North America and Europe and the result of these drives are put on websites (the GPS location of the access points are put on the sites). One common theme that came out from these drives is that at least half of the access points don't even have the basic WEP security on. Guaranteed that WEP is not very secure, still it is enough to dissuade a casual person from prying or getting into the network. In the next section we talk about some simple measures that can be taken to protect the wireless network.

7. Protecting your wireless network

Given the fact that wireless network are much more insecure than their wired counterparts, we need to be more careful with them. Some of the recommendations to help safeguard your wireless network from attacks are listed below.

1. Enable WEP and keep changing the shared key on a regular basis. Select 128-bit encryption if your wireless card supports it.

2. Disable beacons on your access point. Beacons are enabled by default and this means that your access point is broadcasting its Server Set Identifier (SSID) to the entire world, making it easier for any client to associate with the access point.

3. Change the default SSID. The default factory setting SSIDs are readily available on the Internet for most card manufactures. So even if your access point is not broadcasting beacons, it is still easy for a hacker to guess your SSID.

4. Use MAC level filtering. Almost all access points allow you to create a access table and only cards having MAC addresses present in the table are allowed onto the wireless network. MAC addresses can now be spoofed but still this MAC filtering is enough to thwart off casual hackers.

5. Disable Dynamic Host Configuration Protocol (DHCP). Instead of assigning dynamic addresses to the clients, assign them static IP address based on their MAC address.

6. Place your access points away from the exterior walls or windows. Get a wireless expert or determine yourself the best position (maybe, center of the building if using a unidirectional antenna) to place the access points so that the chances of data leakage are minimal.

7. Place a firewall between the wireless LAN and the wired network. You should regulate the traffic exchanged (perform appropriate filtering) between the two networks, so that the corporate data is not compromised even if someone sneaks into the wireless network.

8. Use Virtual Private Network (VPN). Using VPN, all the data will be encrypted and it will safeguard the network from intruders. A tunnel is created between the client and the VPN gateway and it provides a secure passage.

9. Periodically audit your wireless network. Use some of the wireless tools to performing auditing on a regular basis. These tools will help you to find out the signal strength outside the building, any rogue access points or clients that happen to be around (either inside or outside the building – not all attackers are outsiders).

10. Use 802.1x authentication. Have a RADIUS server that will authenticate your clients to the wireless networks. This also provides a means of dynamic key management and a per packet message integrity check.

8. Conclusion

In this paper, we have discussed wireless networks (mostly 802.11b networks) and the dangers that they pose. Because the wireless networks are so easy to set up, they are growing at an incredible pace and will continue to do so for the next few years. The security provided by the wireless network can easily be compromised unless we make a conscious effort to safeguard them. We have listed some of the common measures that one should take to protect their wireless network. Defense in depth is an important paradigm in the world of information assurance. What it means is that we should have multiple layers of protection for our network, so that if one layer is breached, the security implemented in the other layers will help prevent the data from being appropriated. Just like companies implement defense in depth strategy to safeguard their wired network, likewise similar measures should be taken for wireless networks. Wireless networks are not a liability but rather a blessing, and by taking appropriate security measures, we will be able to enjoy its benefits.

9. References

[1] IEEE, “Wireless LAN MAC and PHY specifications”, 1999, 450 pages

[2] IEEE, “Wireless LAN MAC and PHY specifications: High Speed PHY in the 5 GHz band”, 1999, 82 pages

[3] IEEE, “Wireless LAN MAC and PHY Specifications: Higher Speed PHY Extension in the 2.4 GHz Band”, 1999, 89 pages

[4] B Bing, “Measured Performance of the IEEE 802.11 Wireless LAN”, LCN’ 99, Oct 1999 pp. 34-42

[5] Steinkuhler, “Understanding the benefits of IEEE 802.11”, 10 pages, http://www.steinkuehler.de/wavelan_802_11_Benefits.htm

[6] Andren, “CCK Modulation Delivers 11 Mbps for High Rate”, 1998, 11 pages

[7] Z Zuo, “In-building Wireless LANs”, Dec 1999, 16 pages, http://www.cis.ohio-state.edu/~jain/cis788-99/wireless_lans/index.html

[8] Texas Instruments, “New IEEE 802.11g draft standard a win for WLAN market offering 802.11a data rates in the 2.4 GHz band – includes TI’s 22 Mbps technology”, Nov 2001, http://www.ti.com/sc/docs/news/2001/01201.htm

[9] WepCrack, http://wepcrack.sourceforge.net

[10] P Roshan, “802.1x authenticates 802.11 wireless”, Sept 2001, http://www.nwfusion.com/news/tech/2001/0924tech.html

[11] A Frank, “Wireless LANs up-shift to 11 Mbps”, 2000, 5 pages

[12] PersonalTelco, http://www.personaltelco.net/index.cgi/WirelessSniffer

[13] A Mishra, W Arbaugh, “An Initial Security Analysis of the IEEE 802.1x standard”, Feb 2002, http://www.cs.umd.edu/~waa/1x.pdf

[14] J Walker, “Unsafe at any key size: An analysis of the WEP encapsulation”, Oct 2000

[15] W Arbaugh, N Shankar, Y Justin Wan, “Your 802.11 Wireless Network has no clothes”, March 2001, http://www.cs.umd.edu/~waa/wireless.pdf

[16] Wi-Fi Alliance, “Wi-Fi Protected Access Overview”, http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

[17] E Messmer, “Microsoft, Cisco prepare for PEAP show”, 4 pages, Sept 2002, http://www.nwfusion.com/news/2002/0923peap.html

10. List of Acronyms

BPSK	Binary Phase Shift Keying
CCK	Complementary Code Keying
CRC	Cyclic Redundancy Checksum
CSMA	Carrier Sense Multiple Access
DPSK	Differential Phase Shift Keying
DBPSK	Differential Binary Phase Shift Keying
DHCP	Dynamic Host Configuration Protocol
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
FCC	Federal Communications Committee
FHSS	Frequency Hopping Spread Spectrum
HR/DSSS	High Rate Direct Sequence Spread Spectrum
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Group
IDS	Intrusion Detection System
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
IV	Initialization Vector
LAN	Local Area Network
MAC	Media Access Control
OFDM	Orthogonal Frequency Division Multiplexing
PEAP	Protected Extension Authentication Protocol
PHY	Physical
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
SSID	Server Set ID

TKIP	Temporal Key Integrity Protocol
TTLS	Tunneled Transport Layer Security
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access