An introduction to Wireless Networking and the best practices for securing it.
Mark Green
GSEC Practical v1.4b
January 15, 2003

Abstract

The purpose of this document is to discuss the threats to an IEEE 802.11-based Wireless LAN (WLAN) and the best methods for securing your information over that network The paper will begin with a brief introduction of the 802.11 standards, and then cover the different methods of securing the WLAN including explaining the use of WEP (Wired Equivalent Privacy), their shortfalls, and what can be done to harden your WLAN to make it safer for everyday use. Some of the techniques mentioned in this document will most likely be too involved to implement in a home environment but will prove to be an adequate security measure for the small to medium sized business environment.

Introduction to WLAN and its insecurities

Back in 1997 the IEEE (Institute of Electrical and Electronic Engineers) ratified standards 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).[1] In 1999 the IEEE added 2 subsections to the original 802.11 standards, 802.11a and 802.11b.

1. **802.11a** - an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.[2] The purpose of this standard was to create a higher speed wireless technology.
2. **802.11b -** (also referred to as *802.11 High Rate* or *Wi-Fi*) -- an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet. [3] This is the more popular of the 2 technologies and is used in most devices today.

Proposed for ratification in early 2003, 802.11g will be the future of wireless networking. The specifics are as follows.

[1] IEEE 802.11 Standard – "A 802.11 Planet Definition"
URL: http://80211-planet.webopedia.com/TERM/8/802_11.html

[2] IEEE 802.11 Standard – "A 802.11a Planet Definition"
URL: http://80211-planet.webopedia.com/TERM/8/802_11.html

[3] IEEE 802.11 Standard – "A 802.11b Planet Definition"
URL: http://80211-planet.webopedia.com/TERM/8/802_11.html

3. **802.11g –** uses 802.11b's Complementary Code Keying (CCK) to achieve bit transfer rates of 5.5 and 11Mbps in the 2.4 GHz band. In addition, 802.11g adopts 802.11a's Orthogonal Frequency Division Multiplexing (OFDM) for 54Mbps speeds but in the 2.4 GHz range. Success fully combing both earlier versions to provided both speed and flexibility through backward compatibility.

Today Wireless Local Area Network (WLAN) devices based on the 802.11b standard are one of the hottest technologies available on the market today. If you walk into any Electronic Superstore you will find a great many different products that will allow an untrained user to inexpensively establish a WLAN in their home or small office. Consequently most individuals that establish a WLAN do not implement any security to help protect their information. Wireless devices come standard with WEP encryption; although not perfect it at least provides a foundation to build on. When trying to secure a WLAN network there is no one technology available today that can safely accomplish this task. In fact every different method of securing your network mentioned in this document will also have its weaknesses addressed as well. Consequently some or all of the different procedures outlined in this document must be combined if one is to secure the information transferred over the wireless network from wireless eavesdropping.

Threats to WLANs

Today most people with any interest in Wireless LANs have heard the term Wireless Sniffing or war-driving as its most commonly referred to. However not all threats to WLANs are comprised of people trying to hack in. Some of these threats are as simple as radio frequency interferences, or plain improper configuration. To combat these threats the rest of this document will address the proper setup and security to protect your Wireless LAN.

Radio Frequency Interference (RFI)

The 802.11b or Wi-Fi devices as specified earlier use the 2.4 GHz range. The current restrictions imposed by the F.C.C allow for only 3 non-overlapping channels in North America. If the airwaves were entirely clear, three separate switched network segments could operate in the same space. However, the air at 2.4GHz is anything but clear. The band was originally intended for Industrial, Scientific, and Medical (ISM) use-a sink for waste radiation thrown out by microwave ovens, therapeutic heaters, and radar.[4] Also since the 2.4GHz is an unlicensed frequency many different electronic devices such as cordless phones and Bluetooth devices are now transmitting on that band. All this can interfere with the proper communication between clients and Access Points on the WLAN.

[4] Dornan, Andy. "Why Wi-Fi Will Die". Network Magazine.com. http://www.networkmagazine.com/article/NMG2002071S0017.

Proper configuration of an 802.11b device

One of the main selling features of the devices available today is the ease of setup “out of the box”. In the beginning this can be extremely helpful as it means that most wireless cards can be setup by physically installing them in the computer and letting Plug and Play do the rest. Although this is a great idea to get started, it will lead to problems down the road. As each model of Wireless card or Access Point is provided with a specific set of well documented settings it requires little to compromise your default settings. That is why the first step to securing your wireless network is implementing WEP.

Hacking the Wireless LAN

One method of bypassing security and accessing information since the advent of the Local Area Network is the capturing or sniffing of data being passed between the different workstations on the network. This is more of a threat to people using Wireless LANs because you no longer need to physically connect to the LAN to accomplish this. Instead any laptop or Palm-type device equipped with a Wi-Fi card and the appropriate software can accomplish this. Software like Airsnort and Netstumbler are freely available on the internet. That is the main justification for implementing the security settings in this document.

WEP- it’s only the beginning

A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicality’s of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.[5] WEP is based on the use of an RC4 encryption algorithm which is a symmetric algorithm that relies on a single shared key that is used at one end to encrypt the information (plain text) into what is called cipher text, send it across to the far end and then decrypt it. It does this by using either a 64bit or a 128bit per-frame key. The per-frame key is a combination of a pre-shared key of either 40bits or 104bits and a pseudo random 24bit initialization vector. The

[5] Wired Equivalent Privacy - “A Webopedia Definition”
URL: http://www.webopedia.com/TERM/W/WEP.html

initialization vector is randomized for every packet to ensure that every packet has a different RC4 key. When this is combined it creates the keystream. The computer then performs an exclusive OR (XOR) logic function against the plaintext message to create the cipher text. (See FIG. 1 below) The initialization vector is then transmitted in clear text with the cipher text. Once the far end receives the packet all that needs to be done to reverse the process is combine the initialization vector and the pre-shared key to generate the key stream that was originally used to encrypt the data. The receiver in turn runs an XOR logic function against the cipher text with the key stream to recover the plain text.

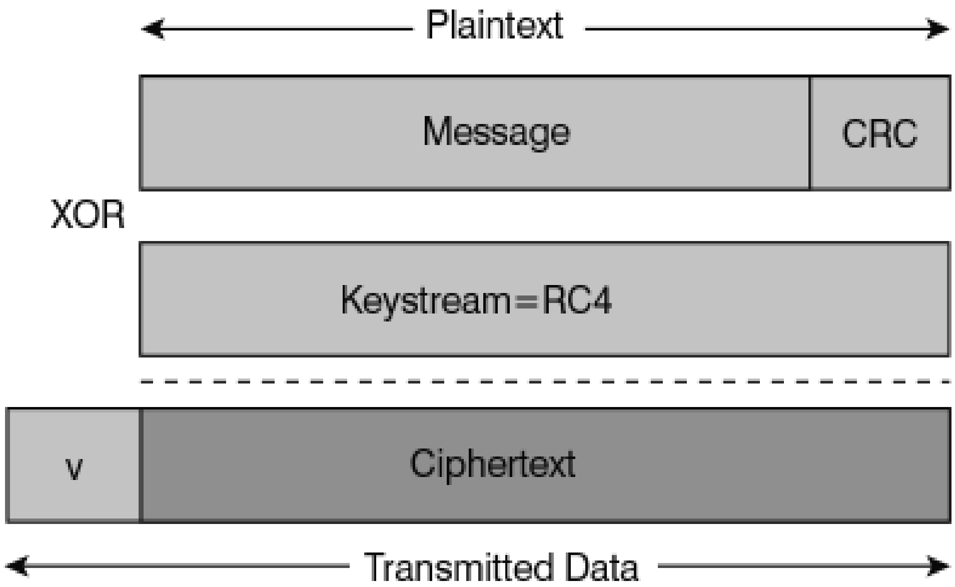

Figure 1: Encrypted WEP frame

Unfortunately, an attacker can capture these frames possessing the plaintext, cipher text, and the initialization vector used to turn the plaintext into cipher text. This is enough information to derive the RC4 keystream—the stream of bits XORed with plaintext to generate cipher text. Capturing a legitimate initialization vector and key stream allows the attacker to successfully respond to any future challenge, without knowing the actual shared key. The attacker has a free pass to join the wireless LAN.

Authorized MAC Lists

Some wireless access points (APs) let you build a table of authorized Media Access Control addresses. MAC Addresses are unique fingerprints provided as part of every wired/wireless network card. This increases the level of security of your network by rejecting any unauthorized wireless cards. Although this small step requires the user to add each card to the authorized MAC table, it will however add an extra layer of security to your wireless network. Unfortunately, the use of a MAC List as a security measure by itself does not provide adequate privacy since MAC addresses are easy to sniff as they are transmitted in plaintext. All an attacker needs to masquerade as a legitimate station is a wireless Network Interface Card (NIC) operating in promiscuous mode for capture with a configurable address to enable spoofing.

Service Set Identification (SSID)

One method that has been implemented in the past is SSID. SSID is an identifier attached to packets sent over the wireless LAN that functions as a "password" for joining a particular radio network. All radios and access points within the same Basic Service Set (BSS) must use the same SSID, or their packets will be ignored.[6] SSID was not originally designed to be used as a method of securing your Wireless LAN; however if the SSID is kept secure by removing it from the access point's broadcast beacon then it effectively becomes an additional level of security.

Secure Socket Level (SSL) Encryption

An additional security measure that can be combined with the previously discussed topics is SSL encryption. For example, if the stations need to interact only with Web sites or Web-based applications (including file and print services over HTTP), then installing certificates on your Web sites to enable Secure Sockets Layer (SSL) is sufficient. If you run more traditional client-server applications that communicate with a Microsoft SQL Server database, change the transport protocol to one that supports encryption (e.g., select the Multi-protocol setting). If users of wireless stations send and receive email through SMTP, POP3, or IMAP4, force the stations to use those protocols over an SSL connection or issue certificates to users so that they can encrypt email messages. And you don't need to secure communications between wireless stations and domain controllers (DCs), because ordinary traffic, including authentication, is already secure—unless your DCs also act as file, print, database, Web, or application servers.

Virtual Private Network (VPN)

In a standard LAN/WLAN combination even with the implementation of any or all of the security measures mentioned earlier in this document the Wireless AP still becomes a way to bypass the firewall and get access to the information inside. (See FIG. 2.) Wireless networking's core deficiencies are in the areas of authentication and encryption. Wireless APs generally perform very little, if any,

[6] Service System Identification – Definition provided by the Wireless LAN Glossary
URL: http://www.wireless-nets.com/glossary.htm

user authentication. If a user is within range of your AP and you're not using any type of security, he or she is connected to your network. WEP provides some value but has numerous inherent flaws. So here's a pop quiz: Which type of networking technology can authenticate users coming from an untrusted space and encrypt their communication so that someone listening can't intercept it? The answer is a VPN.[7]

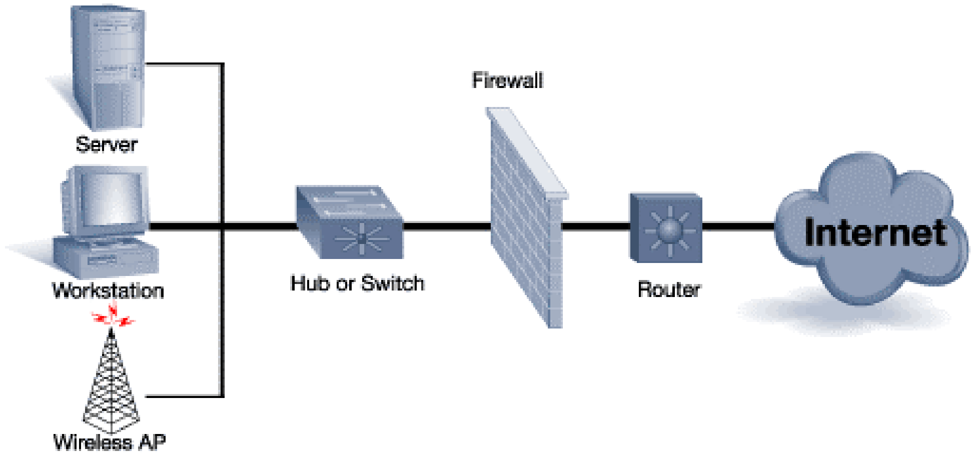

Figure 2: A typical wireless implementation

A VPN is a readily available technology; it does not require any proprietary hardware to implement and can be deployed using almost any server OS available today. But for the purposes of this document I will be discussing the implementation of a VPN using a Windows 2000 Server.

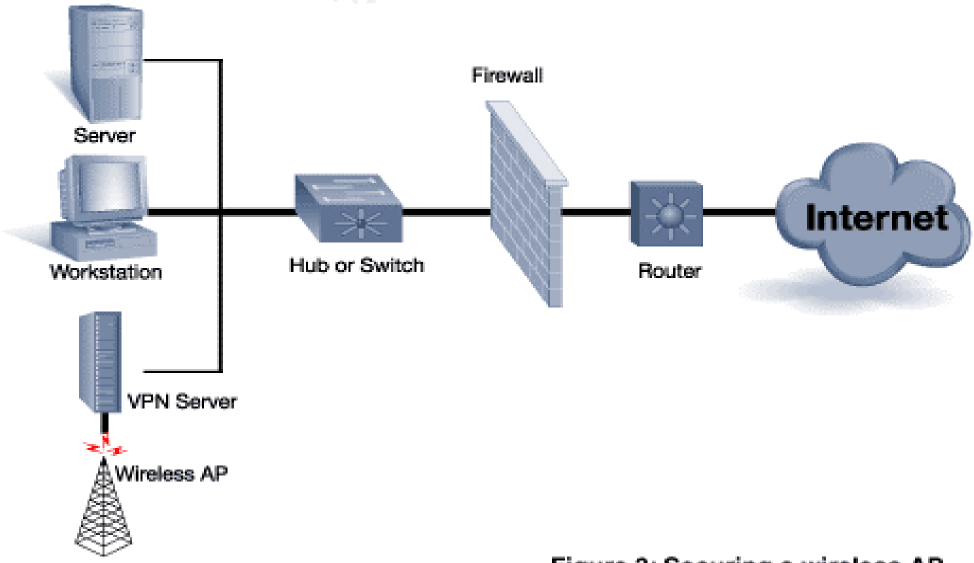

Figure 3: Securing a wireless AP

[7] Use a VPN for Wireless Security - Protect yourself from inherent AP risks
URL: http://www.mobile-and-wireless.com/Articles/Index.cfm?ArticleID=27095

Granted this technology will prove to be more difficult to configure Therefore unless it becomes an included option in the lower priced Wireless APs it will probably not be implemented in the home based Wireless LAN. Using a VPN to connect your Wireless AP to the internal network creates an additional layer of encryption and provides a secure portal to the internal network. Meaning that if a hacker successfully bypasses every other security precaution taken; they will only have access to have access to the computers attached to the Wireless LAN and none of the information stored in the internal network. In this case the internal networks to become like a veritable safe.

To setup the VPN as shown in the diagram (Figure 3) a little planning must be done before attempting the implementation.

1. Choose or build a server to act as your VPN gateway.
2. Add a second Network Card to that server.
3. Choose an IP address range or subnet for the un-trusted network.
4. Configure the VPN Gateway server.
5. Setup the client software on each of the computer allowed through the Gateway
6. Make sure the users that will be connecting through the VPN have the proper access connect to the server

The next phase is the software configuration of the server side of the VPN. This can be configured by using the Routing and Remote access wizard in Windows 2000 Server. To begin the configuration open up the wizard and select VPN server, specify TCP/IP as the protocol required for this server, and the new NIC Card that was added for this connection. Next you must select the IP Address assignment range for the remote clients. Remember to choose the "From specified range of addresses" option. This NIC Card will now become the un-trusted interface. Make sure the only thing that is plugged into this interface is your Wireless AP. The VPN server will now be the gateway to your internal network. Take advantage of your wireless APs DHCP server to provide addresses from your chosen un-trusted subnet that you chose earlier to the computers connecting to this AP. This should complete the server configuration of the VPN installation.

Now each computer that will be connecting to the Wireless AP must be configured to allow for authorization to pass through the VPN gateway. This is done through the Network Connection Wizard. You must specify the VPN gateway by selecting the option "Connect to a Private Network through the Internet". During this setup you will be asked what the IP address of the VPN Gateway is, make sure you specify the un-trusted address of the VPN server and not the address of you Wireless AP.

Once this has been completed you must start the Dial-Up Networking (DUN) connection and provide an appropriate username and password to establish the connection in the logon box. Your system will then establish the VPN connection and authenticate you to either the local accounts database on the server or the Active Directory. Once your workstation has been authenticated by the internal network you can verify the connection by opening up a command prompt and typing in the "ipconfig" command. If your workstation has successfully connected to the internal network you will see both an un-trusted and a trusted IP address.

Internet Protocol Security (IPSEC)

Many security organizations and consultants recommend the use of VPNs to secure WLAN installations, but VPNs can be costly to deploy correctly and can create bottlenecks in your infrastructure. An easier and less expensive alternative exists—IPSEC policies. If you administer or are planning to deploy a Windows 2000 WLAN, you can use IPSec and Win2K Group Policy to provide security without the added cost and potential bottlenecks of a VPN.[8]

Like the VPN method of securing the WLAN this method also requires considerable setup on the network side to prepare for implementation.

1. Choose a dedicated subnet for your wireless network
2. Choose another subnet dedicated for your servers
3. Create a separate Organizational Unit (OU) in the Active Directory for the accounts of all the computers that use Wireless Access cards.
4. Create another separate Organizational Unit (OU) in the Active Directory for the accounts of all the servers that need to be accesses by the wireless network

Next you must create a station policy; this must be done if you plan to apply a server policy to your DCs. If not the server policy will prevent the DCs from communicating with the stations. To create a station policy select the OU created for the wireless stations in Active Directory Users and Computers and create a new Group Policy Object for this OU. It is recommended by Microsoft that you create a new IPSEC policy instead of relying on one of the generic IPSEC policies available. Once this has been completed you must do the same for the OU that contains the Server, this will be the server policy. Now you must run through the security wizard to assign the specific address subnets that were decided on earlier to the security policy and to specify rules that you want in place. On the last page make sure the check box specifying that you want to Edit Properties then click finish. The New Rule Properties box will open automatically. Go to the Connection Type tab and select LAN as the connection type. After this has been completed, you must close the policy to save it, and then it must be applied. To make sure the traffic has been encrypted by the new policies that you have created, open up Network Monitor on the Win2000 Server. Do not be surprised if you continue to see unencrypted traffic between your computers,

[8] Securing Wireless Networks - Use Win2K IPSec policies to protect your WLAN
URL - http://www.mobile-and-wireless.com/Articles/Index.cfm?ArticleID=23374

because IPSec secures IP traffic between end systems, some network traffic—principally non-IP traffic such as Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP)—goes unencrypted. To prevent such traffic, you must use static IP addresses for each wireless station and use ARP commands to manually map IP addresses to MAC addresses.

Conclusion

It was once said that "All things come with a price"; in this particular case hopefully that price will not be the loss of important data due to the configuration or lack thereof of this wonderfully convenient technology. As hopefully demonstrated in this document particular care must be taken in the implementation of any Wireless Network. Because wireless technology is very easy to setup the temptation always exists to just pull a Wireless Access Point "out of the box", plug it in and walk away. Hopefully this document has laid out specific reasons on why special care must be taken before doing so. The short amount of time needed to adequately secure your wireless network is a small price to pay for the convenience that it brings. That being said as with any type of Network the security in place is only effective if it is kept up-to-date. Every day there are new technologies being developed to either secure or bypass the security of your wireless network, so please treat this document as a starting point to any Wireless implementation.

References

[1] IEEE 802.11 Standard – "A 802.11 Planet Definition"
URL: http://80211-planet.webopedia.com/TERM/8/802_11.html

[2] IEEE 802.11 Standard – "A 802.11a Planet Definition"
URL: http://80211-planet.webopedia.com/TERM/8/802_11.html

[3] IEEE 802.11 Standard – "A 802.11b Planet Definition"
URL: http://80211-planet.webopedia.com/TERM/8/802_11.html

[4] Dornan, Andy. "Why Wi-Fi Will Die". Network Magazine.com.
http://www.networkmagazine.com/article/NMG2002071S0017

[5] Wired Equivalent Privacy - "A Webopedia Definition"
URL: http://www.webopedia.com/TERM/W/WEP.html

[6] Service System Identification – Definition provided by the Wireless LAN Glossary
URL: http://www.wireless-nets.com/glossary.htm

[7] Use a VPN for Wireless Security - Protect yourself from inherent AP risks
URL: http://www.mobile-and-wireless.com/Articles/Index.cfm?ArticleID=27095

[8] Securing Wireless Networks - Use Win2K IPSec policies to protect your WLAN
URL: http://www.mobile-and-wireless.com/Articles/Index.cfm?ArticleID=23374

Carney, William. "IEEE 802.11g New Draft Standard Clarifies Future of Wireless LAN." URL: http://www.securitytechnet.com/resource/hot-topic/wlan/802_11g_whitepaper.pdf (23 June 2002).

Interlink Networks. "A Practical Approach to Identifying and Tracking Unauthorized 802.11 Cards and Access Points." Revision C. URL: http://www.interlinknetworks.com/graphics/news/wireless_detection_and_tracking.pdf (3 August 2002).

Lawson, Stephen. "Wi-Fi group lays out better wireless security" URL: http://www.infoworld.com/articles/hn/xml/02/10/31/021031hnwifi.xml?s=IDGNS

Klaus, Christopher W. "Wireless LAN Security FAQ"
URL: http://www.iss.net/wireless/WLAN_FAQ.php

Kapp, Steve. "802.11: Leaving the Wire Behind". On the Wire. January/February 2002. URL: http://www.computer.org/internet/v6n1/w102wire2.htm (3 August 2002).