Doug Baker

December 1, 2003

Security in Wireless Networks

Summary

This paper will describe the Security standards used in Wireless Networks and recommend what I should buy to set one up one of these networks at my house. I'll first cover a few reasons behind wireless technology, explain the standards, discuss the security that was designed into the specifications and what security vulnerabilities are inherent in these standards. I'll then discuss the next phase of wireless security and perform simple market survey to determine what I should buy for my needs.

Introduction

While looking into setting up a wireless LAN in our home I became aware of the numerous security features that the equipment manufacturers were advertising. As I was reading and learning, one feature in particular, Wired Equivalent Privacy (WEP) caught my eye as a feature I'd like to learn more about. Luckily, I also had this report to do so I thought I might as well kill two birds with one stone and complete my practical assignment on this topic for my SANS course. In this paper I'll uncover what security vulnerabilities can be found in Wireless Networking, how secure it really is, and ultimately what do I really need to set up a secure home wireless network

Background

We have multiple computers in our home like a lot of families these days. Like most we only have one printer and one Internet connection that we need to share. So, if I am writing my SAN's report and my wife wants to use the Internet, I have stop what I am doing and let her get on-line. Luckily it's relatively easy to share the Internet connection since our primary computer has an ethernet port and both machines have Windows XP™ as their operating system. In the 'Advanced Properties' tab for our normal Internet dial-up, Internet Connection Sharing has three check boxes that should be selected to allow other machines directly connected to share the Internet connection. While the setup is easy, we are hindered by the length of our Cat-5 crossover cable. So sitting in front of the TV with the Laptop connected to the Internet is possible though somewhat cumbersome with a cable attached. Plus having the cable draped across the floor through the house presents a tripping hazard and the annoyance of getting it out and putting it away every time we want to use it. Investing in permanent connections all throughout the house would be expensive and time consuming. Plus, when all is said and done, change is inevitable. We could rearrange our furniture and block where the network connection was installed. Of course businesses face this same problem on a much larger scale. The cost to establish a permanent local area network infrastructure is very high due to the materials and labor costs required.

Wireless connectivity provides a number of benefits. First it allows us to be truly mobile with our laptop, adding another device requires only a simple transceiver. Also change is not a problem. The cost of the equipment to provide this network is very reasonable and getting cheaper every day.

Its amazing how more and more devices and activities are becoming wireless these days. From reading utility meters from the street to using remote cameras to see who is at your front door, wireless connectivity is spreading quickly. Wireless networking is becoming very common and the service is being provided at numerous public places such as at local coffee shops or while traveling at airports.

The Wireless technology goes by a few names, Bluetooth, Wi-Fi (Wireless Fidelity) and a number of IEEE 802.11 standards. I plan to concentrate on the 802.11 standards since they are the most common standards for what I want to do in setting up a Home Wireless Network.

Background – Wireless Networking

Before trying to understand the security in 802.11 Wireless networks it would be good to understand how they work and where they fit in the big network picture. So first I'll provide background to work from. It is assumed that the reader has an understanding of the OSI seven-layer model and basic knowledge of the Ethernet standards. Using these, as can be seen in Figure 1, the 802.11 specification fits into the overall IEEE 802 (Ethernet) family. The 802.11 specification covers the Physical and part of the Data Link Layers. In the Physical layer, the Wireless devices connect with each other over specified frequency bands defined in the 802.11 standard using low powered transmitters and receivers. The peak data rate between devices is 54 Mbps. In the Data Link Layer the standard then defines the methods how devices are authorized to access the network. The standard also defines the security mechanism used to protect the communications and the network

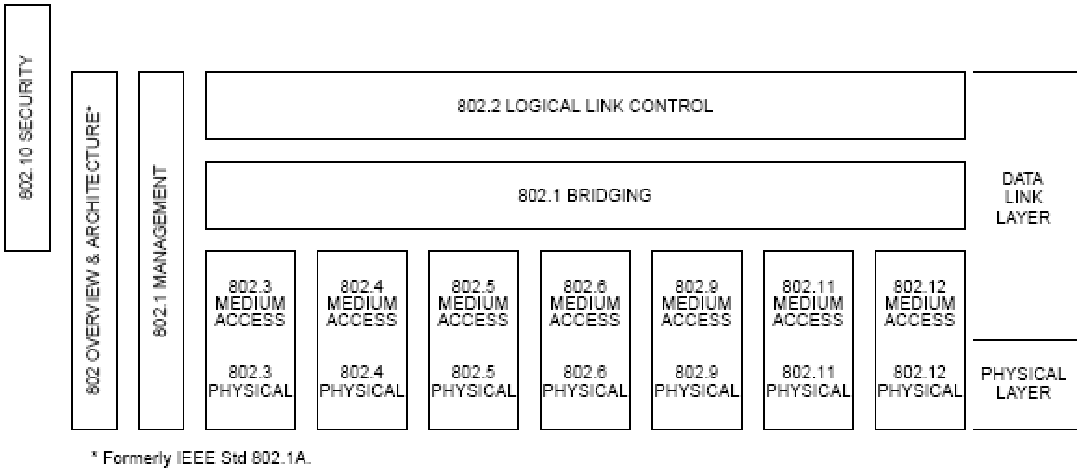

Figure 1. IEEE 802 Family of Standards – Taken from ANSI/IEEE Std 802.11, 1999 Edition

Typical wireless network configurations, as shown in Figure 2, require a mobile or portable station and an access point (AP). The access point is the device that provides the interface between the wireless devices and the rest of the network. The stations initiate the communications by sending out a probe and if there is an the access point that receives the request it will respond, authorize the connection and, if approved, allow data to pass between the two units and to the upper layers of each device.

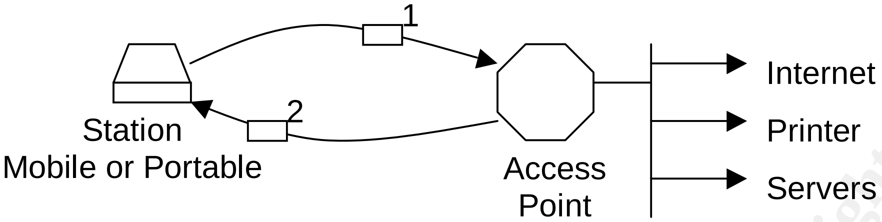

Figure 2. Typical Wireless Configuration

As usual, standards are always changing to meet the needs for more performance or to address a critical shortfall in the existing specifications. The table below provides information on the current standards. The maximum throughput will vary depending upon receive signal strength and number of users in the network.

Standard	Max Data Rate	Frequency Band	Max Users	Compatibility
802.11a	54 Mbps	5 Ghz	64	Dual Band
802.11b	11 Mbps	2.4 Ghz	32	802.11g and Dual Band
802.11g	54 Mbps	5 Ghz	64	802.11b and Dual Band
Dual Band	54 Mbps	2.4 Ghz & 5 Ghz	64	All

Figure 3. Table of Wireless Standards

Wireless Security or Lack Thereof

The 802.11 Standard provides two mechanisms; encryption and Authorization to address the three basic security principles; Confidentiality, Integrity and Availability.

First, wireless networks are inherently vulnerable. There is almost no way to protect the transmissions from being captured. Physical Security is non-existent for these signals due to the very nature of the wireless omni-directional transmissions and the way they propagate in seemingly every direction. So intercepting these signals is simple. Anyone with a wireless receiver, a good directional antenna and widely available freeware can intercept the signals and attack them. Also, there is very little that can be done to prevent someone from trying to get into the network via the access point. Just as you can't limit where the transmissions end up, you can't easily block them from being received.

So how do the standards address these vulnerabilities? First they provide Authentication to manage access between the station and AP to prevent unauthorized users from gaining access. Also, to protect the data, the standards provide Encryption to hopefully make the transmissions unusable.

Authentication

The 802.11 standard specifies two mechanisms for Authentication; Open Authentication and Shared Key Authentication. Open Authentication will grant any request for Authentication. This method is mainly used to allow quick network access and for handheld devices. Shared Key Authentication only allows access to stations with the same key as the AP. In this process the station and AP need to configure a common static web key. The client initiates the connection and the AP sends unencrypted text, which the station encrypts and sends back to the AP. Then the AP decrypts the message and compares this to what is originally sent. If they match, the station has been authenticated and data flow can begin.

802.11 Security also defines the use of a Service Set Identifier (SSID) to limit access. Imagine multiple wireless networks that have overlapping coverage areas. When a station transmits a probe to initiate a connection, multiple AP's would receive it and could respond. It is then possible to join the wrong network. To differentiate the different networks, each should have its own SSID. If the station sends the correct SSID, the AP will recognize it and know its part of the network and continue authentication.

Another method used by some manufacturers to limit access is via Medium Access Control (MAC) address filtering. MAC address filtering is used to augment shared and open authentication. The Access point only allows stations with the correct MAC address to communicate.

Encryption

Now once the station has been authenticated, data will begin to flow. Again, since the data is broadcast, anyone with easily available equipment can view it. So to protect the confidentiality of the information, the 802.11 protocol includes an optional encryption mechanism. The encryption is known as Wired Equivalent Privacy (WEP) and is based upon the RSA RC4 algorithm. WEP is a symmetric stream cipher. Symmetric ciphers use the same key to encrypt and decrypt. The encryption process is also very efficient meaning that it is possible to encrypt and decrypt quickly not requiring lots of processor power or causing a great deal of latency into the data flow.

WEP uses a 64 and 128 bit Seed key length for encrypting the data. Of this, 24 bits are an Initialization Vector and 40 or 104 bits are the secret key. The initialization vector changes from frame to frame and the secret key is static. The initialization Vector is exchanged between the AP and station to increase the effective code length of the Seed Key. Figure 4 below shows how the Secret key and an Initialization Vector are combined to generate the seed key. The Seed Key is created by appending the Secret Encryption Key with the IV. These are then used to trigger the WEP pseudo random generator (PRNG). This output is XOR'ed with the plaintext which has an Integrity Check Value appended to the end. The ICV is used on the receiving end to insure the data sent does not have any errors.

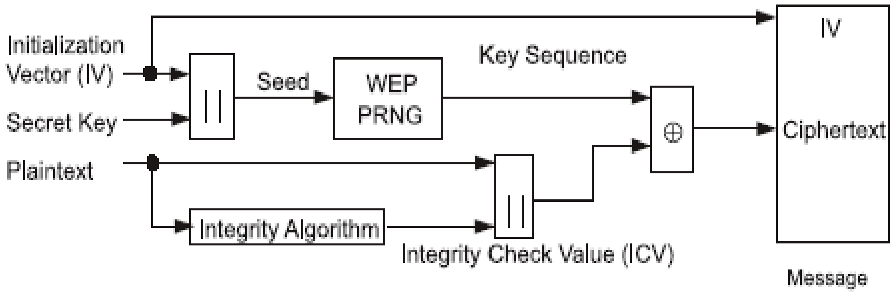

Figure 4. Encryption Process – Taken from ANSI/IEEE Std 802.11, 1999 Edition

The output of this function, ciphertext, then has the IV appended to the front of the frame and the packet is transmitted. Figure 5 provides a representation of the encrypted frame that is sent. As can be seen, only the data and ICV are sent encrypted. On the other side this process is reversed as shown in Figure 6.

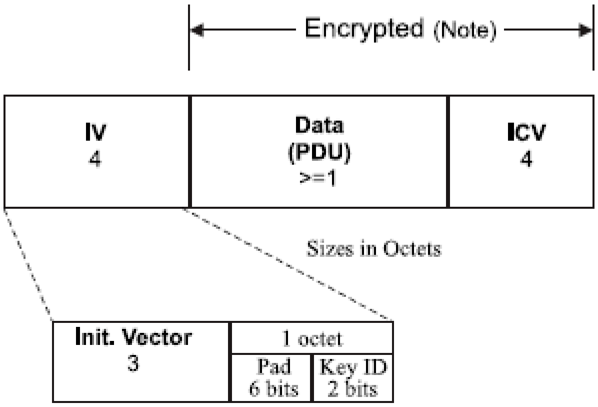

Figure 5. Transmitted Frame - – Taken from ANSI/IEEE Std 802.11, 1999 Edition

In the decryption process the Initiation Vector is stripped off and combined with the secret key again and fed in the PRNG that creates the Key. This is XOR'ed with the remaining part of the message to produce the plaintext and the ICV which was originally appended to the end of the message

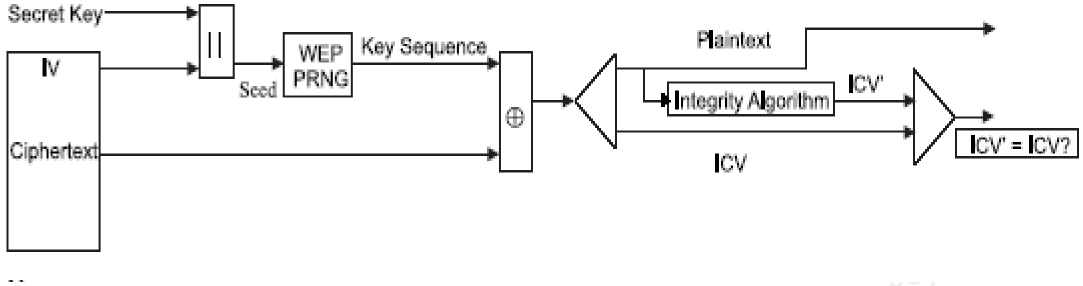

Figure 6 Decryption Process – Taken from ANSI/IEEE Std 802.11, 1999 Edition

Vulnerabilities and Workarounds

Since the 802.11 standard and the equipment have been in use for a while a number of vulnerabilities have been recognized and made public. A few of them are detailed below and what can be done to limit the impact.

- During the Authentication process, the SSID is transmitted in clear text. All that would be required to obtain this is a standard 802.11 receiver and some readily available sniffer software. With this variable, an intruder could easily become part of the network if no other security mechanisms were in place.

  To limit the impact of this, users can change the SSID often or insure the other security features available are used. It would also be good to review the history log on the Access Point regularly to see what or who is accessing the network.

- With Shared Key Authentication, the AP sends a plain text message that the station is required to encrypt and send back. The man in the middle can intercept both messages and perform a brute force attack to try and generate the secret key.

  To limit the impact of this, users could change their secret key on a routine basis. This will require the attacker to be constantly working to attack your network. Making this process harder for an attacker may convince them to attack some other network that is not working to improve the security of their network. If there are easier targets out there, then yours might just be left alone.

- The Initialization Vector used to increase the seed key length is sent in the clear between the station and AP. This process negates any benefit it provides since attackers can easily obtain the number. This also effectively reduces the key length by 24 bits.

  There is not much that can be done to counter this vulnerability since it is inherent in the spec. The best answer is to develop good security practices of using all of the other security features and by changing the key routinely as discussed in the previous bullet.

- Using the MAC address to augment Authentication has a severe weakness in that this is also sent in the clear. This can be easily read and allowing an attacker duplicate the address from their station.

  Again this is inherent in many manufacturers' implementations of 802.11. One option users have against this vulnerability is to track the history log from the AP and correlate this with the known users and their work times. Also, users could provide a verbal request to gain access from the AP owner and the MAC address could them be allowed. Unfortunately, this could require a lot of effort.

- There is no user Authentication, just simple machine authentication for the station. If someone were to 'borrow' the machine, they would have unfettered access to the AP and the network.

  One way to address this concern is to implement user logon's to the machines that have access to the network if possible. Also users should be logged of machines after 10 minutes or less of inactivity.

- The RC4 algorithm used in WEP is an Electronic Codebook type encryption. This means that the same plaintext always generates the same cipher text. This opens up the WEP to a number of other attacks.

  As discussed above, one way to address this is to change the secret key often.

- Bit Flipping Attack. An attacker can duplicate a message then resend it with random bits in the payload changed. This will cause a known error response that the attacker can intercept. Knowing what the plaintext is the attacker can then collect these frames and use them to try and determine the key.

  Same as above, the users should change their key often. Also, the other security features should be used to provide extra roadblocks to attackers.

- Brute force attack is also a known problem. In 2001 three cryptanalysts were able using statistical analysis to derive the WEP key by just passively collecting frames.

  Again, the same as above, change the key often, implement the other security roadblocks and make your wireless network harder target when compared to the rest.

The last and most common problem with wireless network security is with users who use default values when setting up their Wireless network and those who don't use any encryption. Obviously, this makes the network extremely vulnerable. While there are known vulnerabilities with 802.11 Authentication and Encryption, when these are not used or taken lightly, it just makes it a lot easier to attack the network.

There have been numerous cases in the news lately about attackers gaining access to wireless networks. From the November 11, 2003 Detroit Free Press, two men reportedly gained access to the national network of Lowe's through a store in Southfield, MI. Once in the network the guys reportedly altered the software Lowe's uses to process credit cards and installed a malicious program that disabled several computers. Reportedly they just sat in their car in the store's parking lot and gained the access from there.

This kind of activity has become very common and the act of doing this has gotten its own name, Wardriving (http://www.wardriving.com). Folks drive around in their cars equipped with a laptop and a wireless LAN card looking for wireless networks to attack. In a number of the articles describing where this has been done, a large percentage of the networks found had no security mechanisms in place and the Wardrivers were able to join a number of networks. A quick Google search on Wardriving will show some how widespread this activity has become.

So, if a company like Lowe's being attacked and with Wardrivers constantly on the prowl, using the wireless security features is a must no matter if there are vulnerabilities. The attackers will go for the easy target, those who decided to skip the security section of their owner's manual.

Making Wireless More Secure

To counteract the known vulnerabilities in 802.11 equipment, security in higher layer protocols can be used. For example, Virtual Private Networks can be established between the machines using IPSec to secure the communications between the access point and the station. This, in concert with User Authentication, will address many of the vulnerabilities with 802.11.

The Latest

But luckily, the industry has been working to fix these problems for us. Now that the security risks of the 802.11 specification and WEP are well documented, a new standard has been developed to improve security in wireless networks. Wi-Fi Protected Access (WPA) has been developed and is a new standard that provides significant improvements over WEP as detailed below.

First off WPA uses a better encryption scheme, Temporal Key Integrity Protocol (TKIP) to encrypt the plaintext. Unlike WEP, WPA uses dynamic session keys in enterprise solutions and unique passwords for SOHO solutions. In addition the key length is a minimum128 bits.

Also vastly improved is Authentication. For Enterprise setups WPA uses the IEEE 802.1X Authentication with one of the Extensible Authentication Protocols. These are widely used and are known to be secure. These will require that an Authentication Server be connected to the AP to validate user credentials.

In SOHO environments, WPA uses a Pre Shared Password Key (PSK) that is manually entered on client devices and the AP. It uses the same TKIP encryption and provides for Per Packet key construction.

As can be seen, WPA addresses the security flaws with WEP. It uses stronger and dynamic encryption scheme and it provides for user Authentication.

As usual, there are vulnerabilities. One vulnerability in WPA is with the PSK for SOHO environments. Since humans will be establishing this password, it can be susceptible to a dictionary attack. To counter this, users will need to use strong passwords and change them routinely.

What's a New User to do??

Well, now that we are armed with all this information, what should people who are in the market today (like me) go out and buy? WEP or WPA? To add a little more confusion, WPA2 is scheduled to come out early next year, which will be the official IEEE standard. WPA is just the Wi-Fi® answer to fix WEP. Well luckily, WPA and WPA2 are to be backward compatible, so any purchase today should be compatible with the new standard.

So for the SOHO environment, which I am in, what should I be looking for in today's market. Well, WPA appears to have numerous advantages but is it available in the market place? Here is what I found:

Unit	Standard(s)	Security	Cost
Microsoft 2.4GHz Wireless Base Station Model: L21-00001	802.11b	64 and 128 bit WEP	$119.99
Netgear 2.4GHz Wireless-G Router with 4-Port 10/100 Switch Model: WGR614	802.11b and 802.11g	64 and 128 bit WEP	$89.99
Microsoft 2.4GHz Wireless Base Station Model: L21-00001	802.11b	64 and 128 WEP	$79.99
Motorola Wireless Access Point, WA840G	802.11g &b	WPA, & WEP Encryption	$129.00
Proxim ORiNOCO 802.11A/B/G Gold ComboCard	802.11a, b & g	WPA Ready	$99.94,
OfficeConnect Wireless PCMCIA Card - 802.11g	802.11b &g	256 bit WPA, 64&128 bit WEP	$54.95

While searching on the Web, products that came with WPA already installed were hard to find. Many models were advertised as 'WPA ready' which would require an upgrade at some point in the future. So, what is should I buy??

In comparing price, the few devices that WPA installed were not much more expensive than WEP only models. Also, 802.11g is another feature that is nice to have as it is also compatible with 802.11b standard and has a much faster data rate.

So, I can get an Access Point for $79.99 and a PCMCIA card for our Laptop for $54.95. For about $135 plus shipping I can start a simple wireless home network that will be secure and should last me a long time.

List of References

1. http://www.bluetooth.com/tech/works.asp

2. Keeping Your Wireless Network Secure
   By Craig Ellison, PC Magazine
   http://www.extremetech.com/article2/0,3973,1335945,00.asp

3. http://commerce.motorola.com/cgi-bin/ncommerce3/ProductDisplay?prrfnbr=257235&prmenbr=126&bcs_cgrfnbr=230509&zipcode

4. http://www.wi-fi.org/OpenSection/index.asp?TID=1

5. 802.11 WEO: Concepts and Vulnerability, by Jim Geier. http://www.wi-fiplanet.com/tutorials/article.php/1368661

6. Understanding Basic WLAN Security Issues, by Jim Geier. http://www.wi-fiplanet.com/tutorials/article.php/953561

7. PC Client Helps Those Desperately Seeking Wi-Fi, by Jim Louderback. http://www.pcmag.com/article2/0,4149,1252915,00.asp

8. November 11, 2003, Detroit Free Press (www.freep.com), Waterford men hacked store files, FBI alleges, by David Ashenfelter. (Link no longer available)

9. IEEE Standard 802.11, dtd 1999. (www.ieee.org),

10. Picking the Right Topology, by Dave Salvator, http://www.extremetech.com/article2/0,3973,1335950,00.asp

11. Wi-Fi Protected Access (WPA) Need to Know – Part II, by Tim Higgins. http://www.smallnetbuilder.com/Sections-article50-page1.php

12. http://www.wardriving.com/