Global Information Assurance Certification Paper

Securing Wireless Networks

GSEC Certification Practical

By Brett Thorne

November 20, 2004

Introduction

To many people wireless security is an oxymoron. Can it even be secured? The answer varies depending on the level of security that you need. For the average home user, yes a Wi-Fi network can be secured. To a corporation that is negotiating millions of dollars of information a day the prospects are much less promising.

The purpose of this paper will be to introduce you to the world of Wi-Fi security as is it pertains to the home user and small business implementation. We will start off in the first section “Introducing wireless security” with a brief introduction to world of Wi-Fi security. We will show you some comparisons between wireless and the wired networking, and then move into tying it all together as it pertains to security. Next we will talk briefly about the concept of layering your security, in the “Defense in Depth” section. Here we will go over how the defense in depth principle uses multiple layers of security, to build a strong and robust network. The next section “Strengthening your WLAN” will dive into the common vulnerabilities and challenges that are inherent with Wi-Fi and how to mediate and lower the risk factors that are present. Finally in the section “Tools – Hacking your own network” we will look at some of the tools that hackers will use against your wireless network in order to gain access to your WLAN. We will look at a tool call Netstumbler and how the details of this application can greatly increase your security stance.

Recent Statistics

According to America Marketing Institute, the number of Small businesses using wireless LANS will increase by 28 percent in 2004.[1]

Richard Stone, HP's Wireless Mobility Manager states that in terms of cash-money savings, Wi-Fi networking is 30 percent cheaper than "pulling copper wire" for a standard Ethernet network.[2]

Of 500 firms recently polled by Jupiter Research, less than half have implemented security solutions for their wireless networks.[3]

According to Steve Rampado, a senior manager of enterprise risk services for Deloitte and Touche LLP, 30% to 40% of ISACA clients do not change the configuration of their service set identifier (SSID), which is in essence the name of the network. In one other instance, Rampado said 80% of his clients have installed out-of-the-box wireless routers on their internal networks.[4]

Geoff Davies, managing director of i-sec, a British security consultancy says, an informal survey revealed that 67% of the networks they found had the built-in encryption system turned off.[5]

[1] Simonds, Lauren. "Step Up to Wireless Networking." 28 May 2004.
URL: http://www.smallbusinesscomputing.com/webmaster/article.php/3360721 (15 Sept. 2004).
[2] Simonds, Lauren. "Step Up to Wireless Networking." 28 May 2004.
URL: http://www.smallbusinesscomputing.com/webmaster/article.php/3360721 (15 Sept. 2004).
[3] Ellison, Craig. "Keeping Your Wireless Network Secure." PC Magazine. 6 October 2003.
URL: Http://Extremetech.com/article2/0,1558,1312946,00.asp (15 Sept. 2004).
[4] Loffus, Jack. "Small changes can thwart WLAN hackers." 30 June 2004.
URL: http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci991036,00.html (15 Sept. 2004).
[5] Cohen, Beth. "Network Security Basics: Tightening Down Your Wireless LAN." 20 June 2002.
URL: http://networking.earthweb.com/netsecur/article.php/1369391(15 Sept. 2004).

Introducing Wireless Security

Securing a wireless network (Wi-Fi)[6] is very different from the typical wired network. While many of the same principles apply, there are a great deal of new challenges and threats that arise in a wireless environment. The wired network has been around for decades and has had years of growth and maturity. The same is not true for Wi-Fi. With its recent introduction into the consumer market, wireless technology still has a ways to go before obtaining the same level of performance as the wired network – especially when it comes to security.

As the speed of the internet increases and the cost of wireless networking equipment drops, Wi-Fi networking is naturally going to increase in popularity. There are many pros and cons to each of the wiring mediums for networking. For the home and small business implementation, wireless has some very nice features. Let's take a look at how wireless networks compare to cabled networks in terms of setup, etc, etc…

Wireless vs. cabled networks

Up until the introduction of Wi-Fi, in order to connect multiple PC's and other peripherals together required the use of cables (copper or fiber). Now through the use of wireless technology, building your home or small business network can be done with very little money, knowledge and expertise. While both the wireless and the cabled networks require planning and forethought, the cabled network tends to be more sensitive to these concepts and requires more attention to detail when going through the design phase. Here are a few common questions to ask yourself when building out your network.

- ✓ Who will do the work, in-house or outsourced?
- ✓ Is the network going to be setup in an existing building or is it being built from the ground up?
- ✓ Who will design and build the network diagram?
- ✓ Will your network increase in size?
- ✓ Who will support and maintain the network?
- ✓ How much money do you want to invest?

While all of the questions listed above are equally applicable to both wireless and the cabled network, the answers to these questions are far more critical when designing your cabled network. Due to low cost, the lack of wires, jacks and wiring closets, Wi-Fi networks are far more dynamic, so change to the network can be made very quickly and with little redesigning. It is possible to buy various lengths of cable and a cheap switch or hub and throw together a cabled network, but this is neither safe nor secure. Though traditional networking with cables is not difficult, it is still beyond the scope of the

[6] An abbreviation introduced by the Wi-Fi Alliance. The term Wi-Fi is short for wireless fidelity and is used to describe a wireless environment (i.e. 802.11, network, security, etc…)

average user and usually requires the aid of a professional, whether it is to build the cables or design and build the entire network.

Mobility/ Flexibility
Wired networks are limited to the reach of the wires that connect them. Without the use of cables, the network takes on a whole new dimension. Suddenly all the rooms in the company or home become a part of the network environment. Existing buildings no longer require expensive redesigning and custom build outs. Networks can be built up and torn down in a matter of hours rather than days. This adds a great deal of flexibility to conference rooms, client offices and war rooms. Whether you're working in the lounge area of your business to working in the front room of your home, mobility and flexibility are some of Wi-Fi networks greatest features.

Speed
Here is where a Wi-Fi network clearly falls short of the wired network. With a wired network, data throughput speeds vary from 10mbps to 1000+mbps at the desktop. In the world of Wi-Fi, throughput speeds typically peak at 22+mbps. Theoretical speeds vary from manufacture to manufacture but are rarely hit on a consistent basis. Wi-Fi is currently not suited to high bandwidth environments.

Price
Price is one of leading reasons small business and home users are jumping on the Wi-Fi movement. Yes it is newer technology and this is always very exciting, but cost is really the bottom line. Running and building wires, network designing, support, maintenance and remodeling all increases the cost of the overall network structure and business overhead. With the low cost of Wi-Fi technology, the small business owner can now have the same dynamic flexibility of networking his/her business without having to spend the large corporate costs.

Security
Security is very difficult to place a pro or a con to. For example if a small business or home user requires Wi-Fi only to do work remotely once in a while when performing business presentations or doing school work, Wi-Fi security is probably going to be more that adequate. But on the other hand to an end user that is performing bank transactions or payroll, a cabled network may be the most secure. Wi-Fi implementation and its intended use in the home or business will determine whether or not it will be secure enough for that application. At the current level of maturity that Wi-Fi is at, it is simply not as secure as a wired medium.

Wireless vs. Wired

	Wireless Network	Wired Network
Install & Setup	X	
Mobility	X	
Flexibility	X	
Price	X	
Security		X
Speed		X

To summarize, a wired network is more difficult to install, setup and change, but provides the best solution for security and speed. On the other hand Wi-Fi networking is very easy to install, setup and change, but does not have the security strength nor the speed of a wired network.

Tying it all together

We have talked briefly about the pros and cons of Wi-Fi networking, but how does this all tie into security? Due to the ease and cost of installing, we are seeing more and more Wi-Fi networks pop up in the home and small business sector. Typically these installations are being done by individuals that do not understand the complex nature of securing the wireless environment. Though wireless networks have advantages in setup, flexibility and price, and have adequate throughput for many environments, they have to have sufficiently strong security to be useful in the ever changing world of the Internet. With all the advantages that Wi-Fi has to offer, there is one significant disadvantage over a wired network - Security. It's interesting to point out that the very thing that makes a Wi-Fi network so easy and dynamic to work with is its very downfall, the lack of the network cable. With the use of cabling you gain a far greater level of privacy than you do over a wireless medium.

Defense in Depth[7]

What is Defense in Depth? In a nutshell it is applying multiple layers of security to your network environment. This may include: servers, desktop PC's, Operating Systems, Printer, Wi-Fi networks, etc…

The Defense in Depth strategy has been best described using the analogy of an onion. At the core of an onion lie you critical data. From the core there are multiple layers of the onion, each representing a layer of security. This may include firewalls, virus protection application, OS updates, encryption, etc…For each layer of security protection you use the greater the chances of you preventing an attack, locating it and defending against it. Each layer standing on its own serves very little protection, but as a whole the sum of the entire security implementation stands as a much stronger defense strategy.

The concept of using multiple layers of security blends perfectly with Wi-Fi networking. All the features that add to the overall security of the network will each be enhanced by each other as then are implemented together.

Typically hackers will go for the weakest network. Why try to get into a network that will take hours when there is one next to it that will only take minutes or even seconds. Just a little security can take you a long ways and may prevent the passerby hacker from hitting your network. With the principle of Defense in Depth your goal is to be the network that is passed up because of the level of security implemented. Let's take a look at these different layers as they apply to wireless security.

[7] Cole, Eric., Fossen, Jason., Northcutt, Stephen., Hal Pomeranz. Defense in Depth 1.2. SANS: SANS 2004. 11 – 64.

Strengthening your WLAN

Now that you have an idea of what the Defense in Depth strategy is and how it's structured let's now take a look at how to apply it.

There are many areas of weakness inherent with Wi-Fi networking. Most of the items that we will discuss are easy to overcome while others are more difficult and require special equipment to secure. It is important to reiterate that each of the security steps listed below, acting alone will not secure your WLAN. By applying multiple levels of security (defense in depth) you will have a much stronger foundation for securing your network.

Let's take a look at some of these vulnerabilities.

- ✓ Changing the Default AP Details
- ✓ Disabling the SSID Broadcast
- ✓ Enabling Encryption
- ✓ Enabling MAC Address Filtering
- ✓ Installing Firewalls
- ✓ Virtual Private Network (VPN)
- ✓ Antennas & Signal Strength
- ✓ War Driving/War Chalking
- ✓ Hardening Wi-Fi PC's
- ✓ Maintenance
- ✓ Education is KEY!

Changing the Default AP Details

It was pointed out earlier in recent statistics that a great deal of Wi-Fi users have installed out-of-the-box wireless routers on their internal networks.[8] This out of the box configuration makes it easy for a hacker to access your router. Finding the default settings on a router is trivial at best and can easily be circumvented if not changed. There are many websites available that have lists of all the default settings found on the various brands of AP's. Changing the default name and password of the AP should be one of the first steps in the Defense in Depth strategy. Be sure to change the default AP name and password. When changing the password be sure to use a strong password that includes uppercase, lowercase, numbers and special characters. Make sure to limit the amount of DHCP Users that connect to your network. For example if your network requires 3 PC's to connect to the network, limiting the range from 192.68.1.1-3 will give you just the amount of connections needed. Having more connections that is needed only increases your exposure. This figure can always be changed later if more connections are needed. Finally, make sure that you change your AP IP Address to a different subnet. In most cases you can use 192.68.1-254.*

[8] Loffus, Jack. "Small changes can thwart WLAN hackers." 30 June 2004. URL: http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci991036,00.html (15 Sept. 2004).

Disabling the SSID Broadcast

By definition "Short for service set identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the AP."[9] The SSID is used to identify your Wi-Fi network, similar to a network name in Windows. Whenever a user wishes to connect to the Wi-Fi network they will need to know the SSID. By default, most Wi-Fi AP's broadcast this SSID out like a beacon, several times per second. Knowing the name of the network is the first step to being able to hack it. It is always a good practice to turn this feature off. While disabling this feature alone will not protect your WLAN it could however prevent the passerby hacker from easily gaining access to your network.

Enabling Encryption

Encryption is one of the most overlooked security defense in the Wi-Fi environment. In a recent study, I scanned 100 WLANs, of the 100 scanned only 3 were using encryption. Almost all your Wi-Fi routers in production today support some sort of encryption. This can vary from 40 bit to 128 bit and even some manufactures claim to have 256 bit encryption available. Enabling encryption varies from vendor to vendor. One thing that they all have in common is the need for an encryption key. For WEP (Wired Equivalent Privacy) this is done by providing a fixed 10 character Hex key length for 64 bit and a 26 character hex key length for 128 bit encryption. WAP (Wi-Fi Protected Access) uses a variable key length from 8-63 bits in length. The HEX key is used by the access point and the network nodes to encrypt and decrypt the data sent back and forth. The longer and more random your key is the better. It is also important to note that frequently changing your HEX keys will increase your security stance. The frequency at which you change your keys will be determined by the importance of the data on the network. Weekly key changes may be adequate for the home user, where daily key changes may be needed for a more secure environment. Most venders provide a utility called a key generator to aid in the process. There are also freeware versions of these key generators as well. It has been discovered that there are flaws in various venders' key generators that actually reduces the effectiveness of your encryption key. Therefore manually typing in your own WEP key using a random set of hex characters will reduce this possible vulnerability.

Let's take a look at the different encryption methods.

WEP (Wired Equivalent Privacy) is privacy protocol specified in the IEEE 802.11 standards to provide protection and privacy against eavesdropping. WEP is typically 64 bit and 128 bit in strength and uses an RC4 standard for generating the key. 64 bit keys are really only 40 bits in strength where by 24 bits are used as the initialization vector or IV. The same is applicable to a 128 bit encryption. 128 bit keys are actually only 104 bits strong and again 24 bits are used as the initialization vector. So WEP Encryption is really not as strong as it sounds and yes there are many more problems with WEP than what we have briefly covered. The point is, is that some form of encryption is better than none. Remember Defense in Depth.

---

[9] Encyclopedia Entry. "SSID." 18 May 2004.
URL: http://www.webopedia.com/term/s/ssid.html (15 Sept. 2004).

WAP (Wi-Fi Protected Access) was developed as part of the 802.11i security specifications to overcome the flaws in WEP. It is designed to be a strong security replacement for WEP and to be software upgradeable to existing Wi-Fi Certified products. WPA provides an improved data encryption by scrambling the keys being used with a hashing algorithm called TKIP (Temporal Key Integrity Protocol). With the use of TKIP, the network gains integrity checking to ensure that the keys used have not been tampered with. WPA also provides user authentication with the use of a protocol called EAP (Extensible Authentication Protocol). It is important to note that if any of the equipment in your WLAN is using WEP and has not been upgraded or configured to use WAP the default encryption standard will revert back to WEP for downwards compatibility. When purchasing your WLAN hardware, make sure that they are upgradeable to the new WAP standard. This will allow for a more secure encryption implementation across your WLAN. The fine details of WAP are beyond the scope of this paper but are worth investigating, for more information on WAP please see References.

Enabling MAC Address Filtering

Every network device contains a MAC address (Media Access Control address, also known as an Ethernet address). This hardware address is hard-coded on the NIC (Network Interface Card) and uniquely identifies one node on the same network segment with another. These 48 bit unique MAC numbers are written in 12 digit hexadecimal format with the first 24 bits uniquely identifying the manufacture or vendor whereby the last 24 bits are used as a unique serial number. No two MAC address should be the same. So what is MAC Address Filtering? It's the process of configuring your AP with a list of MAC address that can be allowed to connect to the WLAN. By placing a hardware devices MAC address on your AP's MAC address filter list you are stating that, that device can now connect to your WLAN. If a device is not on the MAC address filter list and tries to access the WLAN they will be denied. This feature coupled with WEP/WAP encryption makes a significant change in the security of your WLAN.

Installing Firewalls

Firewalls come in all shapes and sizes, from software based products, to hardware ones, and from packet filtering devices, to application-aware proxies. The type of firewall that you choose will vary greatly on the amount of detail and security you wish to invoke. For example: for the home user a simple but robust personal software firewall like Zone Alarm may be enough to cover the needs on the network. However for a small business, protecting valuable data, may opt to use a more extensive product like a dedicated hardware Stateful packet inspection firewall. There are many access points that provide some sort of firewall capability. The strength of the firewall is often times related to the cost. Some AP's provide packet filtering while others provide the more robust Stateful Packet Inspection (SPI). Firewalls allow you to control the traffic flow to and from your WLAN. They can even provide you with valuable information about the traffic that has traveled or has attempted to travel on your network. By default you will want to start by blocking all incoming traffic across the network. Then as needed, open up ports one by one to allow access to the individual applications and users. If your AP

comes with a firewall, it is always wise to enable and manage this feature. Firewalls are a must in the scheme of wireless security.

Virtual Private Network (VPN)

A VPN is a common alternative to WEP for encrypting data over a Wi-Fi network. A VPN is capable of allowing Wi-Fi users the ability to establish a secure point to point connection over a non-secure medium. With the use of a VPN a Wi-Fi user can securely communicate using a much stronger encryption method, typically IPSec. This eliminates vulnerabilities found in the common encryption method of WEP. It was mentioned earlier that WEP keys need to be changed frequently in order to reduce the chances of the keys being hacked. For a large network this can be a significant overhead. Changing the WEP key would need to be done on every node connecting to the Wi-Fi network. With the use of VPN an admin can manage the network centrally making the network admins job much easier. Implementing a VPN is fairly straight forward and requires the use of either a VPN software package, pass-through server or and operation system that supports VPN, such as Windows XP or Linux. Most Wi-Fi AP's provide some sort of VPN support, but it's always a good idea to make sure that the AP that you have chosen will allow this feature set for future expansion. It has been said that the only way to secure a wireless communication is through a VPN.

Antennas & Signal Strength

Antennas can be used for several purposes. There are powered antennas that allow your signal strength to increase in distance and consistency (typically used with access point). And then there are antennas used by the listening devices, such as laptops, PC's etc…that allow you to pickup signals from greater distances. Both work very similar but vary depending on application. So how do they relate to security? Let's talk about two main factors, placement and type. The placement of an antenna has a great deal to do with security. Place your antennas in areas where hackers cannot blend themselves in as employees or visitors. Make sure that your antennas are not placed in areas where signal strength will pass beyond the boundaries of your environment. Try to place you antennas in central locations within your home or office, avoiding outside walls and common walls. Using the wrong antenna can be just as dangerous as its placement. An antenna that is more powerful than needed, will change your private network to a public one by extending your signal well beyond the confines of your home or office. Careful placement and purchase of your antennas will greatly increase the security of your WLAN.

Some AP's allow you to manage and change the signal strength. This is very beneficial in a smaller environment where signal strength can extend beyond the confines of your home or small business. By roaming with a wireless device you can test the signal strength of your AP, reducing it to only those areas that need it. This is an excellent measure for reducing the amount of passerby attacks on your network and is commonly overlooked.

War Driving/War Chalking
Okay war driving/chalking may be a stretch on securing you Wi-Fi network but there are some things we can learn from these techniques. What is the purpose of war driving? Simply put, to find free internet. Okay there is more to it than just finding free internet, but in its simplest form that's really all it is. Performing a war drive on your own WLAN can tell you a lot about how secure your network is. It's free and can be very beneficial. War Chalking is marking a building or landmark where a Wi-Fi network has been located. When a Wi-Fi source has been found it's marked using chalk with one of three symbols. The)(symbol indicates an open node or no SSID being used. The W with a circle around it indicates that WEP is being used. And finally a O indicates a closed node or no SSID broadcast. If you see these markings near you home or business it is recommended that you remove the markings immediately and perform a war driving test on your own network. Chances are you will find that your network is vulnerable.

Hardening Wi-Fi PC's
There is a lot that can be said about PC hardening, so I only want to briefly discuss its importance in the scheme of Wi-Fi security. Hardening a desktop can be a very complex and lengthy process. It can be done by locking down a desktop through profiles, local as well as group policies, to allowing end users full control over the local PC. For our discussion we want to focus on hardening the desktops through a more practical implementation more suitable for WLANs. Here are a few suggestions to hardening your Wi-Fi PC's.

- ✓ Install an Anti-Virus solution
- ✓ Install ALL OS updates (i.e. Service Packs, Security Patches, etc…)
- ✓ Install ALL Application based Updates
- ✓ Implement hardened shares and disable any shares not needed
- ✓ Install Personal Intrusion Detection Systems
- ✓ Install Personal Firewalls
- ✓ Enable Local File Encryption

The list above provides a solid foundation to start your desktop hardening. Your particular needs may vary but you get the point. Adding layers to the desktop further strengthens your stand against malicious behavior and increases your Defense in Depth strategy.

Maintenance
We have covered a lot of various ways of securing your Wi-Fi network. Just as each step covered is critical to securing your network, it is just as critical to maintain your network and to stay on top the ever changing world of Wi-Fi. New technology is being developed daily and more and more vulnerabilities are being brought to the surface even faster.

By performing a few simple maintenance steps you can keep your network up to date and as dynamic as the hackers themselves.

- ✓ Change the password and network name of your access points frequently. By randomly changing your passwords and network name on your access points you will decrease the possibility of an individual guessing these details.
- ✓ Monitor the MAC addresses connected to your network. Check the list of MAC addresses currently connected to your network frequently. This is a great way of detecting rogue devices connected to the network as well as eliminating any devices that may not need the access. Routine maintenance will ensure a clean and accurate network.
- ✓ Cycle your encryption keys often. Once again changing the encryption keys frequently will decrease the chances of an individual guessing or cracking your encryption.
- ✓ Turn off your Wi-Fi network whenever you are not using it. If know one is using the Wi-Fi network, then why have it enabled? Turning off your Wi-Fi network when not in use reduces your exposure.
- ✓ Perform periodic war drives on your network. Depending on the size of your Wi-Fi network, war driving may be a little over done and perhaps war walking is more appropriate. Performing periodic war tests on your network will help in determining holes in your security, hopefully before the hackers do. These tests can be tremendously valuable to your overall security standpoint and should be performed frequently. Changes to the network in the form of upgrades, size increases or decreases, etc… all warrant a war test. Changes to the network can sometimes have an adverse or hidden effect that could open you up to other vulnerabilities.
- ✓ Keep up to date with Virus Patterns. Staying up to date with virus patterns is always a good practice. With the ever changing world of the Internet, PC's, etc… new viruses are being developed daily and old viruses are being modified just as quickly. Frequent updates to your virus software are a necessity and should be a frequent routine in your network maintenance.
- ✓ Keep your OS and Applications up to date with there patches. As quickly as new viruses are being developed, new holes and vulnerabilities in the software that we interact with are being exploited. By staying on top of your patches and updates you will significantly decrease your overall threat level.
- ✓ Audit your PC's for vulnerabilities frequently. Auditing your PC for vulnerabilities varies from free scanners such as Microsoft's Windows Update or Microsoft's Base Line Analyzer to more advanced systems such as products provided by eEye Digital Security or HFNetChk. There are literally hundreds of analyzers to choose from. The type of system that your choose will vary greatly on the importance of the information and type of machine that your are protecting. The point is is that frequent testing on your network and the machines that are a part of the network will help you to find the vulnerabilities before the hackers do.
- ✓ Sign up for multiple security bulletins. The use of security bulletins can greatly increase your exposure to the various vulnerabilities, viruses, hacks and tools that are being developed and exploited daily. By having these details emailed to you daily, you greatly reduce the amount of time spent researching. Here are a few examples:

http://online.securityfocus.com/cgi-binsfonline/subscribe.pl

http://www.us-cert.gov/cas/index.html

http://sans.org/newsletters

Keep up with your maintenance routines often. It's easy to let you guard down when the network is running so well. This is the time that you should be learning about new and up coming technology. This is the time to perform your maintenance on the WLAN. Regular maintenance will not only keep you sharp and a head of the game but your network will be as well.

Education is KEY!

Educate those users that will be working and using the Wi-Fi network. Teach them about the importance of Internet security, proper use of e-mail and the various security measures in place on the network. The more the end users are aware of the importance of security and how it effects the environment that they work in, the easier your job as an administrator will be.

Tools – Hacking your own network

Well we have talked briefly about some of the security measures that a Wi-Fi administrator can take to secure the network, and how adding multiple layers of security adds to your defense in depth strategy. But how can you test these measures? How do you know for sure that your network is secure?

The best way to determine how secure your Wi-Fi network is is by trying to hack into it yourself. Armed with a few simple tools you can gather valuable information about your network and determine just how secure or non-secure your network is.

The most common tools used for hacking into a Wi-Fi network are a laptop with wireless enabled, a mobile Wi-Fi antennae and Netstumbler. The laptop is used for obvious reasons. It's mobile and allows you to perform testing from all areas of the network environment. The Antennae is optional, but well worth the investment. You can build your own antennae for very little money or you can purchase a commercial version. Either one will give you great results. With the use of the antennae you can perform war driving/walking on your own network. This can be done from your car or nearby location (i.e. a parking lot or adjacent building, etc…) or by just walking around. Next is the use of Netstumbler. Netstumbler is a freeware application that allows you to detect various 802.11x networks and there settings. It will provide you with detailed information such as signal strength, AP name, encryption information, SSID etc…Let's take a look at some screen shots of a Wi-Fi network scan using Netstumbler.

Figure 1 shows a Wi-Fi network setup right out of the box. Notice that the SSID is shown and with the default ID of NETGEAR. This is a good indication that the AP has been setup with all the default settings. There are hundreds of sites that contain default settings for AP's that can help reduce the guess work in hacking the network. For example, we know that this AP has been setup with a default SSID and that it is being broadcast. With this information we can assume that the AP is using the default IP and login credentials. For Netgear the default AP IP is 192.168.0.1. With this information coupled with the default User name and password a hacker can easily gain access to the AP and make any changes necessary to aid in his or her attack. Another important fact to point out is the lack of detail in the Encryption column. This indicates that no encryption is being used. What about signal strength? With WEP enabled and the SSID unavailable a hacker can still use a packet sniffing tool such as Ethereal or Airsnort and obtain packets sent over the network. This can provide the hacker with the SSID and the WEP key. As you can see with a simple tool like Netstumbler a lot of information can be deducted, that can aid in a possible attack.

Let's now take a look at a Wi-Fi network setup with a few default changes. You'll notice in Figure 2 that the SSID is no longer being show in the SSID column. This indicates that the broadcast of the SSID has been disabled on the AP. You should also notice that the Encryption column now shows WEP is being used. You can see by using tools such as Netstumbler an administrator can greatly increase the networks defense in depth.

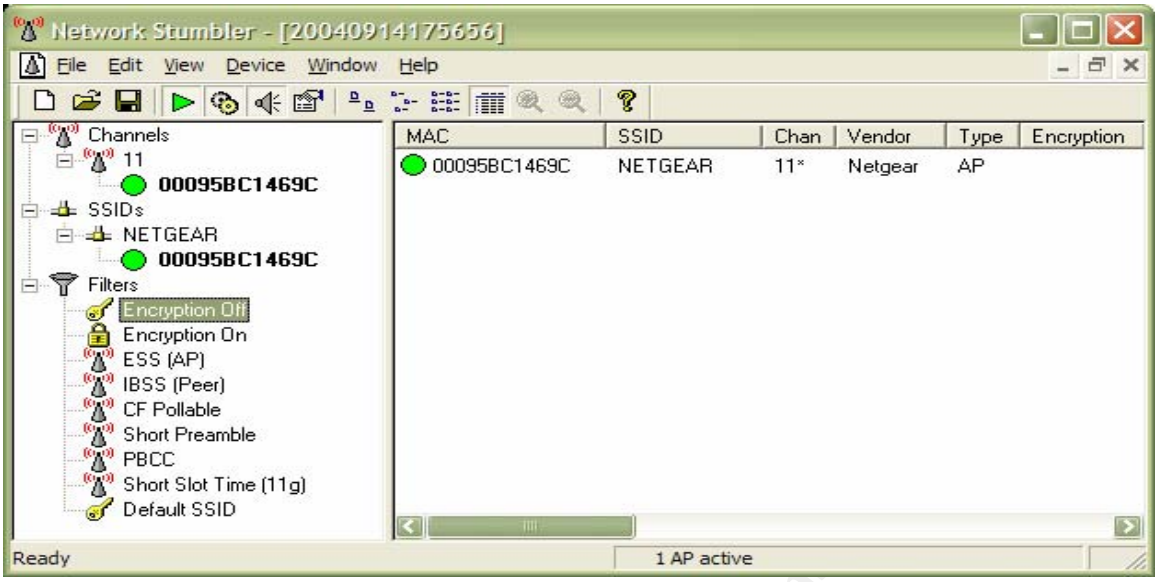

Figure 1

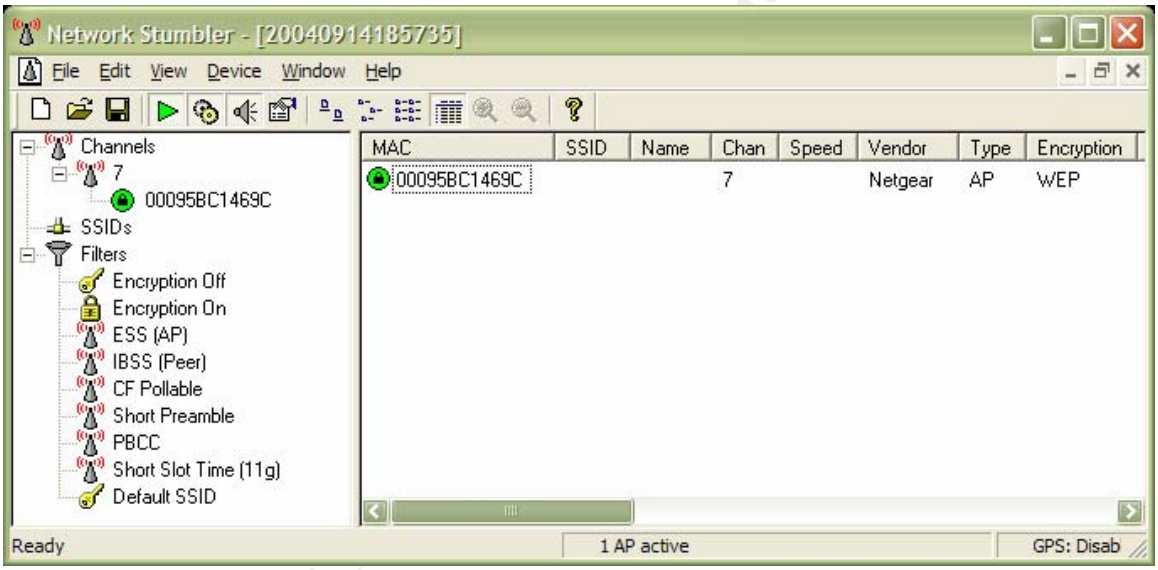

Figure 2

There are a lot of tools and methods for penetration testing that are beyond the scope of this paper. However, it's important to remember that performing these tests and determining the weaknesses in your network up front will save you a lot of time and money. Familiarize yourself with the tools and methods used by hackers so that you can further enhance your own security stand. Take the time to read up on the latest techniques and strategies available. Keep up to date with new technology and always get permission in writing before performing any testing or hacking on the network.

Summary

We talked about some recent statistics that indicate that Wi-Fi is here to stay and will continue to grow at a rapid state for the next several years. This growth fueled by low cost and ease of installation is causing a decrease in network security. We also learned that a great deal of the Wi-Fi networks that are being implemented are failing to follow the most basic of security principles.

Introducing Wireless Security allowed us to discuss the differences between wireless and wired networks and how the two different media types produce various pros and cons between each other. We then compared Mobility/Flexibility, Speed, Price, and Security between Wi-Fi and Wired networks and learned that security was the biggest downfall of the Wi-Fi network. In tying it all together we summarized the various pros and cons and re-iterated the fact that wireless network though flexible and inexpensive requires more attention to security than a wired network environment.

In the Defense in Depth section we touched briefly on the importance of the Defense in Depth strategy and how this played a large part in our security focus. We learned how the Defense in Depth strategy applies multiple layers of security to our Wi-Fi network and how each layer acting on its own was not enough to protect the critical data. The multiple layers of security provide redundancy and backup to each layer before it and after thereby increasing the security stand of our network.

In Strengthening your WLAN we talked about the multiple layers that would build our Defense in Depth strategy. We introduced layers such as changing the default AP details, disabling the SSID broadcast, enabling strong encryption, enabling MAC address filtering, firewalls, and VPN's. We introduced concepts like adjusting signal strength, choosing the right antennas, war driving and war chalking, and hardening PC's. We finished up this section with a brief discussion of maintenance and the importance that is plays in our day to day administration. Finally we finished up with education is the key. Keeping up to date with new technology and teaching the users who will be a part of your network about the importance of security will greatly reduce your risks.

We then ended the paper with a discussion about Tools – Hacking your own network. Here we briefly talked about the tools and methods used in determining how secure or non-secure your Wi-Fi network is. We introduced an application call Netstumbler which allows us to gather valuable information about our network and its vulnerabilities. We then finished up the paper by talking about the importance of learning about the tools and techniques that hackers are using on us. The more we know about them, their skills and tools the better we will be at defending our Wi-Fi networks.

References

Simonds, Lauren. “Step Up to Wireless Networking.” 28 May 2004.
URL: http://www.smallbusinesscomputing.com/webmaster/article.php/3360721 (15 Sept. 2004).

Simonds, Lauren. “Step Up to Wireless Networking.” 28 May 2004.
URL: http://www.smallbusinesscomputing.com/webmaster/article.php/3360721 (15 Sept. 2004).

Ellison, Craig. “Keeping Your Wireless Network Secure.” PC Magazine. 6 October 2003.
URL: Http://Extremetech.com/article2/0,1558,1312946,00.asp (15 Sept. 2004).

Loffus, Jack. “Small changes can thwart WLAN hackers.” 30 June 2004.
URL: http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci991036,00.html
(15 Sept. 2004).

Cohen, Beth. “Network Security Basics: Tightening Down Your Wireless LAN.” 20 June 2002. URL: http://networking.earthweb.com/netsecur/article.php/1369391(15 Sept. 2004).

Cohen, Beth. “Securing the WLAN: Are the Alphabet Standards Finally Soup?” 16 Aug. 2004) URL: http://networking.earthweb.com/netsecur/article.php/3395481 (15 Sept. 2004)

Encyclopedia Entry. “Wi-Fi.” 16 Jan. 2004.
URL: http://networking.webopedia.com/TERM/W/Wi_Fi.html (15 Sept 2004).

Cole, Eric., Fossen, Jason., Northcutt, Stephen., Hal Pomeranz. Defense in Depth 1.2.
SANS: SANS 2004. 11 – 64.

Barken, Lee. “WEP Vulnerabilities – Wired Equivalent Privacy?” 23 Dec. 2003.
URL: http://www.informit.com/articles/article.asp?p=102230&seqNum=9 (15 Sept. 2004).

Definition. “WEP (wired equivalent privacy).” N/A.
URL: http://nwfusion.com/details/715.html (15 Sept. 2004).

Encyclopedia Entry. “WPA.” 18 June 2004.
URL: http://wi-fiplanet.webopedia.com/TERM/W/WPA.html (15 Sept. 2004).

Vaughan-Nichols, Steven J. “Making the Most from WEP.” 6 March 2003.
URL: http://www.wi-fiplanet.com/tutorials/article.php/2106281 (15 Sept. 2004).

McGarvey, Joe. “War(chalking): What is it Good For?” 12 July 2002.
URL: http://www.wi-fiplanet.com/columns/article.php/1402401 (15 Sept. 2004).

Author Unknown. “Wi-Fi Security.” 2004
URL: http://www.weca.net/OpenSection/secure.asp?TID=2 (15 Sept. 2004).

Bradley, Tony., Waring, Becky. “Complete Guide to Wi-Fi Security.” 30 June 2004.

URL: http://www.jiwire.com/wi-fi-security-introduction-overview.htm (15 Sept. 2004).