Global Information Assurance Certification Paper

No Information Security Department? No Problem!
A Practical Guide to Securing Wireless Networks

Eric V. Stewart

GSEC Practical Assignment v. 1.4b – 08/29/2002
ADMINISTRIVIA v. 2.5b – 02/2003

Abstract

Several weekends ago my roommate and I were standing in the check-out line at the grocery store when we saw the cover story on the front of Barron's Weekly (4/28/03), *High on Wi-Fi.* My computer-clueless roommate asked what Wi-Fi was and so, much to my regret, I quickly explained to him that it is the industry standard for wireless Local Area Networks (WLANs), which allows users to utilize high-speed Internet communications over airwaves, much like a two-way radio. This was to my regret because the next thing out of his mouth was "Cool! Let's put Wi-Fi in our house". After beating him over the head with the paper for a few minutes and explaining just how much of a security nightmare Wi-Fi currently presents, he quickly changed his tune.

The whole point of this entertaining little story is that larger companies with sound information security and networking groups will know the hazards that are associated with wireless networking and either; 1) avoid wireless altogether or 2) adopt wireless and do everything within their power to protect the company network and data. On the other hand, most home users and small business owners may not even think about the security issues when considering building their own wireless networks. Many of these individuals are completely blinded by how "Cool" wireless is and how they'll be able to surf the Internet from their backyard while enjoying the sunshine and fresh air.

Introduction

With all of the on-line, magazine and television marketing that Intel and other wireless manufacturers have been conducting as of late for their latest and greatest mobile technology, even the least computer savvy people have to have noticed that the Wireless Revolution has kicked off at an astounding rate.

Wireless hardware prices are plummeting rapidly by the month, thus making WLANs the latest networking rage in both the home and business environments. The hardware required in order to build a WLAN can be purchased for anywhere from $100 on up depending on the quality of the gear (obviously, the more dependable equipment will cost more). The most popular manufacturers of WLAN equipment recently are Linksys, Cisco, 3Com, Intel and Lucent. These manufacturers are leading in market sales due to their ease of hardware installation and product functionality.

WLANs provide users with an escape from fighting with tangled runs of networking cables and phone cords. Rather than being constrained to a desk by a cable, WLAN users can operate from anywhere in their home or small office. If they feel like lounging by their pool while browsing the World Wide Web, then that is exactly what they can do. All of this independence from cables and cords sounds wonderful, but wireless networking does not come without its shortcomings; the biggest being security.

The goal of this paper is to give a high level explanation of the security risks involved with WLANs. I will also cover the different wireless standards, in order to help determine what standard can best meet specific security needs as well as compile a list of best practices

that will help home wireless users and small companies lock down their WLANs. These practices are most effective when they are used in conjunction with each other. Please understand that these practices are *not* guaranteed to make a user's wireless network impenetrable, but each tip creates an additional hurdle between a potential attacker and the user's wireless network and their personal data. Lastly, I will discuss a few of the many tools available on the market today that will help WLAN users discover security holes in their WLAN so that they can fill in those holes and keep their network more secure, because, as they say, it is much better to be safe than sorry.

Wireless Security Risks

To date, very little has been available in the way of security when it comes to wireless networks. This is changing hastily though as many people are realizing the associated security risks. The following are the major wireless networking security risks:

- Unauthorized Access to Network - Attackers may be able to connect to a wireless network for the purpose of connecting to the Internet.
- Eavesdropping - Attackers may be able to intercept wireless data transfers and search them for valuable, personal and/or business information.
- Denial of Service - Hackers may be able to conduct a denial of service attack in which they "keep users from accessing services, either to gain some sort of competitive advantage or just have some devious 'fun'". [1]
- Unauthorized Access to Data - Attackers may be able to connect to a wireless network and gain access to personal and/or business information stored on local network computers.
- Alteration or Deletion of Data – Attackers may gain access to local computers and either destroy or change the data or system files.

For these reasons most industry security experts discourage conducting sensitive personal business, such as credit card transactions, health care business, or finances on a wireless network.

Here is a short example to help bring the understanding of these risks closer to heart. Nearly everyone has, at one time or another, experienced interference on a cordless telephone where they could hear or be heard by a neighbor on a cordless telephone. This is very similar to the situation that could occur with a wireless network's signal. The signal from a wireless network travels almost as far as (up to ¼ of a mile in some cases) that of a cordless telephone and is therefore just as susceptible to being intercepted. Think about where you live. How many buildings are within ¼ mile of your home?

And it's not just other buildings that users have to worry about either. War driving has become very popular lately. War driving is when attackers drive around with their laptops, wireless access cards, and directional antennae looking for rouge wireless signals to exploit. Once an attacker has found an exploitable wireless signal, they may mark the outside of the building, war chalking, for others to exploit.

Wireless Standards

All of the WLAN standards discussed below have been developed by the Institute of Electrical and Electronics Engineers (IEEE). The IEEE is a group of academics, engineers and scientists whose work is directly involved with computers, electro-technology, and all associated sciences. A standard is a benchmark that we may use in order to measure a WLAN's performance and quality against.

According to 802.11 Planet, 802.11 is "a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station". [2] 802.11 is broken down into three principal sub-levels; 802.11a, 802.11b, and lastly 802.11g, which are all described in greater detail below. These 820.11 sub standards are all very similar in basic theory and the only major differences are in rate at which the data is transferred and the frequency bands in which they operate.

802.11b

Probably the most common standard when dealing with home and small business WLANs, 802.11b is considered to be "the standard that started it all" [3] when referring to wireless networking. 802.11b is the original bearer of the "Wi-Fi" name, which it was given in 1999 to avoid sounding too techie. 802.11 operates over three simultaneous frequency channels (of the eleven available in the U.S.) in the 2.4 GHz frequency band at transfer rates up to 11 Mbps within 100 feet of the wireless access point (WAP). The speed will drop off significantly as the user moves away from the WAP, to the point that the speed will be as low as 1 Mbps at 300 feet away.

Considering that 802.11b is the standard that kicked wireless off, it is also the only standard that is currently accepted around the globe. 802.11b equipment can be used whether you're in the U.S., Asia, Europe, South American and Africa, whereas 802.11a and g are only seen in North America and in limited use across Europe.

While 802.11b may seem to be infallible it does have its disadvantages. "Two disadvantages of 802.11b networks are generally slow speeds and the potential for interference in the 2.4MHz band over which they transmit". [4] As you will soon read in the 802.11g section below, 11 Mbps is considered to be slow in terms of today's connectivity speeds. As far as the potential interference is concerned, simple household items can cause signal interference. Signal interference will occur if your WAP or wireless network access card is in close proximity to a microwave oven or a 2.4 GHz cordless telephone.

802.11a

802.11a is the second generation standard of wireless networking to have been introduced. This standard is much faster, nearly 5 times faster, than its predecessor 11b operating at transfer rates up to 54 Mbps in the 5 GHz range over eight available frequency channels. 802.11a and 11b and not compatible as they both operate in

different frequency ranges and this is not to 11a's advantage as the majority of WLAN equipment sold to date has been for 802.11b (Figure 1).

Very similar 802.11b, 11a will also experience reduced transmission speeds as the wireless access card and WAP are moved farther apart. The maximum operating range of 300 feet for 802.11b is much greater than the maximum of 150 feet for 820.11a. Although this reduced operating range of 802.11a may be discouraging to some, 11a has a distinct advantage over 11b in that it does not experience signal interference caused by microwaves and cordless telephones because it operates in a much higher frequency range.

The fact that 802.11a does not experience the same appliance based interference that 11b does and that it has such a high rate of data transfer makes 802.11a very well suited for enterprise level usage rather than for home use. Another benefit of 11a to the enterprise level is its reduced operating range. Enterprises will be able to effectively provide a signal to all of its work areas by using multiple, well placed WAPs. This reduced operating range will minimize having the enterprises wireless signals from spilling out of their buildings into the surrounding areas, thus addressing a major security concern for wireless; signal containment.

802.11g

The third generation standard 802.11g is a combination of both 11b and 11a. Much like its predecessor 11b, 802.11g operates in the 2.4 GHz range over three simultaneous frequency channels (of the eleven available in the U.S.). The 802.11g transfer rates, however, take after 11a and are in the speed range up around 54 Mbps and can transmit up to nearly 1500 feet if the signal is unobstructed. 802.11g is backward compatible with 11b, but not 11a. Backward compatible means that 11g wireless access cards can be used to connect to WLANs using 11b WAPs, but not vice-versa.

"Often thought of as the best alternative between faster 802.11a and the older and slower 802.11b, 802.11g is likely to make the most sense for consumers and small businesses in the future". [5] This standard will be the best choice for small businesses and home users because of its increased speed over 11b and the fact that it is backwards compatible with 11b, which is the most prevalent standard in today's environment. The backwards compatibility is very beneficial as network owners will not have to replace all of their older 11b equipment if the decide to move ahead with 11g network equipment.

The increased data transfer rate does not come without its down side though, as 802.11g is still, much like 802.11b, at a disadvantage when it comes to signal interference in the 2.4 GHz frequency range, due to microwave ovens, cordless telephones and other WLAN equipment operating in this same range.

Dual-Band, Tri-Mode Wireless

This isn't quite a standard in itself, but rather the combination of several standards working as a single, best of all worlds, standard. As I have discussed, the only compatibility between the above discussed IEEE 802.11 wireless standards is the

backward compatibility of 11g to 11b. This lack of compatibility can prove to be very costly for WLAN owners who want to upgrade from 11b to either 11a or 11g. In an effort to minimize the pain, discomfort, and cost of switching standards, wireless hardware manufacturers are now producing dual-band, tri-mode wireless hardware. These components are WAPs and wireless access cards that will support all three IEEE modes, 802.11a/b/g, in both the 2.4 and 5.0 GHz range, all while housed in a single unit.

The pricing of these dual-band, tri-mode components is significantly higher than that of single-band, single mode hardware and may not currently appear to be worth the cost, but in the long run this additional cost will be far out-weighed by increase in WLAN flexibility, stepped up transfer speed and decrease in signal interference from nearby sources. As shown in Figure 1, Allied Business Intelligence, Inc. predicts that Dual-Band 802.11 will be the standard of the future for all of these reasons.

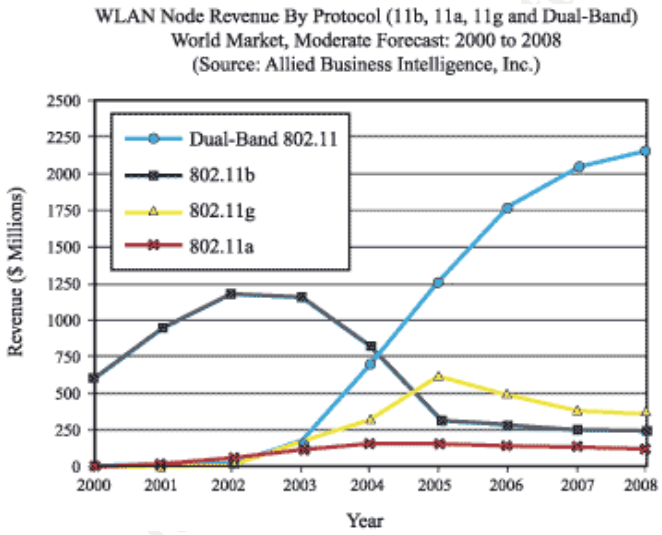

Figure 1 – WLAN Equipment Sales [6]

Best Practices

Just as when dealing with the securing of traditional wired networks, there is no single silver bullet solution or magical configuration setting when it comes to securing a wireless network from attacks and intrusions. The dangers associated with wireless computing and networking can only be *minimized* through a combination of positive wireless computing habits and appropriate wireless networking hardware security configurations.

An 'Onion Method' of security must be applied when attempting to secure a wireless network. That is, the network must have many layers of security, just as an onion has many layers. If you peel off one layer, or break through one security mechanism, there will be many more below that an attacker will have to break through as well. The following are trusted industry security practices for wireless networking that can be used in conjunction to protect WLANs:

Remove or turn off Wireless Network Access Cards when not on-line. I realize that this may seem like it is going a little bit overboard, but if the card is either un-installed or disabled, then an attacker who may gain access to the WLAN will not be able to gain access to that particular computer. In this case, any private or personal files on the computer will be safe from prying eyes.

Limit the number of users who can concurrently access the WLAN if the specific equipment allows. This can be done by setting the allowed number of DHCP (Dynamic Host Configuration Protocol is a network protocol that, using a DHCP server, automatically assigns an IP address to each network computer) addresses able to connect to the WLAN to the number of computers that will be on the network. If all available addresses are already in use, then an attacker will not be able to access the WLAN. On the other hand, if a WLAN user tries to get onto the network but cannot, then this may indicate that an uninvited user may be accessing the WLAN.

Enable 128-bit Wired Equivalent Privacy (WEP) if the specific equipment allows. WEP is limited to IEEE 802.11b and it was designed to offer the same level of security to wireless networks as is associate with wired networks. Wired networks are considered physically secure from outside intruders based upon the fact that they are contained within a building. Wireless networks do not have this same luxury as the wireless signal does not stop once it encounters a wall. The signal penetrates all physical boundaries and is available around the building for anyone to exploit.

The WEP algorithm has been designed "to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network". [7] Unfortunately, as many people in the Information Security industry will argue, WEP is a very weak security feature for wireless networking, but a weak security feature is better than nothing at all. If WEP is to be left disabled, the WLAN is practically wide open for any potential attackers to have their way with.

When WEP is enabled, the WLAN owner should make it a point to change the encryption keys often. The more often these keys are changed, the less likely that someone may guess them. In addition to changing these keys often, owners should make it a point to set difficult to guess keys. Do not use keys that are easy to guess, such as, ABC123, PASSWORD, DECEMBER, or 55555. Changing the keys periodically requires effort and diligence, but is a good security practice.

Control the WAPs broadcast signal if the specific equipment allows. The goal here is to keep the wireless signal from escaping the physical boundaries of the home or small office so that nobody outside can take advantage of any stray signals. Many of today's manufacturers produce WAPs that allow for the fine-tuning of signal strength and even direction of the wireless signal.

In order to ensure that the signal is properly tuned, the WLAN owner can set the signal so that it is accessible from all desired areas within the confines of the building. Once this has been completed, the owner can then walk the outside perimeter of the building, and inside rooms where the signal is not desired, with a wireless enabled laptop to check for signals.

If signals are found outside of desired areas, then the owner can readjust the signal and re-perform these signal checks.

Ensure that all equipment in the WLAN is protected if the specific equipment allows. WAPs and routers from all manufacturers come with default settings that should really be changed upon installation; otherwise the gear may be compromised by an attacker. There are default security settings that are quite generic and not specific to a WLAN's security needs. These settings must be customized so that they are detailed to best protect the specific WLAN.

In addition to the default security settings, all WLAN gear comes with default passwords associated with their 'Administrator' accounts. It is imperative that these passwords are changed upon installation or else an attacker can go through the list of known default passwords and take control of the WLAN hardware. Once an attacker has administrative rights, they can remove all security settings and boost the WAP signal strength for other attackers to ill-use.

Be very cautious when using Service Set Identifiers (SSIDs). Service Set Identifiers (SSIDs) are unique identifiers that differentiate one wireless network from another, so all access points and all devices attempting to connect to a specific wireless network must use the same SSID. There are several security tips associated with SSIDs; equipment default SSIDs, broadcasting of SSIDs, and accepting "any" SSID.

Manufacturers ship their WLAN products with "default" SSIDs. These defaults are the same for all equipment produced by that manufacturer. Attackers can go through a list of commonly known default SSIDs in order to try and penetrate a WLAN, so it is very important to change the default SSID. The SSIDs, just as the WEP keys, should be set to non-obvious settings that will not be easily guessed. Also, it is important to change SSIDs frequently to minimize the chance that they may be guessed.

WLAN equipment has the ability to broadcast its SSID on a periodic basis. The SSID is very easy to intercept because it is broadcast in clear text. This makes it very easy for an attacker to determine the SSID for the particular WLAN, so it is a very good security practice to disable the SSID broadcast if your equipment allows for this. The ability to disable the SSID broadcast is commonly known as the "closed network" feature.

Several manufacturers produce equipment that will accept clients with any SSID. It is important, if the equipment allows this, to disallow the acceptance of any SSID other that that which you created so that only users with the proper SSID access the WLAN.

Limit WLAN access to computer MAC address if the equipment allows. A MAC (Media Access Control) address is a unique identifier assigned to differentiate every network access card worldwide. Seeing as how these addresses are exclusive to each and every card, WLAN equipment can be set to only allow specific MAC addressed network access cards to connect to the WLAN.

Although this solution sounds like a silver bullet solution, it is not. Attackers can still by-pass this security measure by Mac address spoofing, which refers "to an attacker altering

the manufacturer-assigned MAC address to any other value". [8] Although it is highly unlikely that an attacker will be guess one of the authorized MAC address to spoof, it is possible to get via WLAN equipment that hasn't been properly secured (refer to '*Ensure that all equipment in the WLAN is protected'* above).

Take advantage of a Virtual Private Network (VPN). If the equipment allows, use a VPN between all personal wireless computers and the WAPs. "VPNs typically employ some combination of encryption, digital certificates, strong user authentication and access control to provide security to the traffic they carry". [9] This will help to prevent an attacker from seeing any information that is being transmitted by setting up a secured tunnel directly from the computer to the WAP. Use of a VPN will decrease transfer speeds slightly, but when dealing with sensitive data, this is a trade-off that is well worth the security results that will be experienced.

Be very cautious when sharing files on the WLAN. It is very important that WLAN owners do not set their computers to share any more than is absolutely necessary. They should not share any folders that contain personal, medical, or financial information. If it is necessary to share these folders, then password protection should be used on these folders. These passwords must not be set so that they are easily guessed and must also be changed frequently.

Continuously upgrade the network equipment firmware. Firmware is a combination of software and hardware that is built into most wireless networking devices and has data or programs recorded on them regarding hardware operation. Manufacturers continuously release updated firmware and the equipment needs to have its firmware periodically upgraded in order to fix bugs and/or provide new functionality for the device.

WLAN owner should make it a point to update the firmware of all system components from their manufacturer's web site on a regular basis. By doing so, the WLAN's equipment may then acquire new security features. The new feature can then be leveraged in order to assist in securing of the WLAN.

Apply available patches to the operating system frequently. Most operating system manufacturers will release security patches for their software on a regular basis to secure known flaws. While this won't really help prevent attackers from accessing the WLAN, it will assist in preventing the amount of damage that they may inflict during an attack. In addition to added security, installing these patches may also provide added functionality to the operating system. All-in-all it is a no lose practice.

Avoid wireless Hot Spots. Wireless Hot Spots have been popping up all around the country as of late. From convention centers to coffee houses; airports to libraries; hotels to dormitories, they are everywhere. No matter how tempting it may seem though, to cruise down to the local Starbucks and browse the internet on a wireless enabled laptop while enjoying a steaming cup of coffee, wireless users should try at all costs to resist the temptation.

There are currently around 1.7 million hot spot access locations available in the United States and it is predicted that there will be over 20 million hot spot users by 2007. These

Hot Spots use secure mechanisms in order verify subscriber identity and payment method, but that is as far as the security generally goes. [10] Once authorized and paid in full, the user's locally stored information and wireless transmissions are fair game to any near by attackers. Considering the popularity of these Hot Spots, users may be surrounded by wireless attackers and not even know it.

In addition to wireless Hot Spots lacking in the security area, these wireless hot spots do not have a tendency to come cheap either. Prices tend to run anywhere from $5 per day up to $50 per month. If users are already paying for a home Internet connection, it doesn't make sense to pay this much for a hot spot connection that lacks security for sensitive information.

Put to use a client side firewall. While use of a personal firewall, such as Zone Alarm (http://www.zonelabs.com), will not do much to protect your data while being transmitted, it will however protect your data at rest by preventing attackers from getting onto the local network computers and even help to prevent attackers from launching a denial of service attack on those computers. Firewalls can also be quite useful in detecting certain types of malicious software that try to access the Internet.

Utilize NetBEUI for Microsoft Networks File and Printer sharing when possible. Use of NetBEUI as a networking protocol today is not as common as it was in the past since the advent of TCP/IP. Now, almost all networks are running on TCP/IP over NetBEUI. If an attacker were to get access to the WLAN via a non-secured WAP, they would most likely have access to all of the files on the computers running TCP/IP File and Printer sharing. On the other hand, if the network in question were using NetBEUI, the local files would probably be safe due to the use of the superseded networking protocol. Many InfoSec professionals would refer to this practice as 'Security through Obscurity', but I would have to counter that comment by saying that it'll get the job done 9 times out of 10.

Always use virus protection on the WLAN computers. While this may seem obvious, I figure that it is at least worth mentioning because it is just that important, whether connected to a wired or wireless network. Viruses do not care if they are propagating over a wire or an airwave; they will unleash their fury regardless. In addition to personally running anti-virus software, owners should also require that any visitor to access their WLAN is running the most up to date software as well. This way they will be confident that no one will be letting loose any viruses on any of their computers.

Once again, I must reiterate that the fifteen afore mentioned best practices are just that, best practices. Not one of them alone will completely secure your wireless network, therefore it is important to use as many of them as the WLAN equipment will allow. The more the better as each one will act as an additional barrier keeping potential attackers that much farther from the WLAN and the sensitive data contained within it.

Wireless Security Tools

There are many tools available today to help ensure that WLANs are safe from potential hackers and attackers. These tools help owners to find security vulnerabilities so that they can repair them prior to them being exploited. Hackers are using many of these same tools

in order to find ways into WLANs, so why not use them to prevent uninvited visitors from getting access to the network in the first place? Take a look below to learn more about just a few of the many available tools that can be used to test WLAN security. If more information is desired on available tools, http://www.networkintrusion.co.uk/wireless.htm is a valuable site that contains information on over 30 of the available programs that can also be leveraged for WLAN security testing.

Wireless Access Point Detection Tools:
Use of these tools will help WLAN owners and administrators to test their networks to determine if all WAPs are properly secured and signal strength is set as to not transmit out of the desired area.

NetStumbler, a freeware download, available from http://www.netstumbler.com provides the ability to scan the airwaves for and log 802.11b WAPs using a Windows computer. This software is very popular amongst war drivers, but has, in the past, been limited to only to use with ORiNOCO wireless network cards although, the most recent version "supports a whole load of new cards on XP". [11]

AirTouch Network's War Walking Kit, available at http://www.airtouchnetworks.com, is a software and hardware package that also helps to sniff out WAPs. This package comes with a hand held antennae, wireless network card, and all associated software. Using this kit, owners can walk the perimeter of their property or home to ensure there are no rouge wireless signals available for potential attacks.

WEP Cracking Tools:
Use of these tools will assist in verifying that the WEP algorithm on network components has been enabled with a strong encryption key.

WEPCrack, available at http://sourceforge.net/projects/wepcrack, is a Linux based WEP cracking tool that takes advantage of faults discovered in the key scheduling of the RC4 algorithm. Once an attacker has a WEP encryption key, they can read anything that users are pushing across their wireless signal, thus owners want to ensure that they change their keys on a regular scheduled basis.

AirSnort, available at http://airsnort.shmoo.com, is a tool that, via air sniffing, can recover both 40 and 128-bit WEP encryption keys. "AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered". [12] This tool is a very similar to WEPCrack, in that it also exploits known faults in the RC4 algorithm.

ArpSpoof Monitoring Tools:
These tools will assist in finding unsecured networking protocols, which may be leveraged in an attack, so that the vulnerabilities may be remedied prior to any attacks that would leverage these faults.

Dsniff can be downloaded free of charge from http://naughty.monkey.org/~dugsong/dsniff/. ArpSpoofing is when an attacker fools the attacked network into thinking that it is part of the network. Once the attacked network trusts the attacker, there is nothing to stop the

attacker from having access to all information and communications. Dsniff is designed to run primarily on open source operating systems although an older version that will support Windows platforms is available at http://www.datanerds.net/~mike/dsniff.html.

Wireless Traffic Sniffing Tools:
By using wireless sniffers, WLAN owners will be able to monitor their wireless network traffic to verify that it is properly secured and therefore, help to ensure that a man in the middle attack will not occur.

Ethereal, a freeware download from http://www.ethereal.com/, is a network packet sniffer that supports both open source and Windows. Sniffing the network traffic will help the owner to determine if their data is at risk while in transport or if it has been adequately protected. This traffic can be analyzed real time or saved to a file for analysis at a later time.

KISMET can be downloaded at http://www.kismetwireless.net/. This freeware wireless sniffer "is different from a normal network sniffer (such as Ethereal or tcpdump) because it separates and identifies different wireless networks in the area". [13] This feature is rather practical when working in close proximity with other WLANs, so that traffic from nearby networks is not confused as that of the network being analyzed.

Conclusion

In writing this paper, I hope that I have enlightened the reader as to the multiple flavors of WLANs, the security risks involved in wireless networking, WLAN best practices, and available tools that may be used to ensure that a WLAN is effectively secured against potential attacks.

Wireless networking has, to date, been inherently insecure. The security risks associated are not to be taken lightly else valuable data will be put in jeopardy. These WLANs are quite vulnerable, that is unless the proper steps are taken to harden the network. The best practices that I have laid out in this paper are excellent building blocks to be used in securing a wireless network, but please realize that it is crucial to never be satisfied when it comes to securing a WLAN. The securing of a WLAN is a continuous work in progress, as new security risks are discover every day. The goal of every WLAN owner should be to stay on top of these risks so that sensitive data is not compromised.

As I have mentioned earlier, the Wireless Revolution has kicked off at an astounding rate and now the aim is to ensure that wireless security catches up to it.

References

[1] Geier, Jim. “Minimizing WLAN Security Threats”, 802.11 Planet 09/05/2002. 05/19/2003 <http://www.80211-planet.com/tutorials/article.php/1457211>

[2] 802.11 Planet Glossary, 802.11 Planet 12/16/2002. 05/08/2003, <http://80211-planet.webopedia.com/TERM/8/802_11.html>

[3] Anderson, Chris. “The Wi-Fi Revolution”, Wired May 2003. 05/15/2003 <http://www.wired.com/wired/archive/11.05/unwired/wifirevolution.html?pg=2&topic=&topic_set=>

[4] Ohlhorst, Frank J. & Gros, Michael. “Off the Wire”, Entrepreneur May 2003. 05/15/2003 <http://www.entrepreneur.com/Magazines/Copy_of_MA_SegArticle/0,4453,308065----1-,00.html>

[5] Hawn, Andrew. “Digesting Wi-Fi Alphabet Soup”, TechTV 03/10/2003. 05/16/2003 <http://cache.techtv.com/freshgear/products/jump/0,23009,3420326,00.html>

[6] Allied Business Intelligence, Inc**. “**Wireless LAN's Future Is Established As Big Tech and Telecom Companies Enter The Market, According to New ABI Study”, 01/22/2003. 05/15/2003 <http://www.alliedworld.com/abiprdisplay.jsp?pressid=146&filename=wlan03pr.pdf>

[7] Borisov, Nikita, Goldberg, Ian and Wagner, David. “Security of the WEP algorithm”, 05/23/2003 <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

[8] Wright, Joshua. “Detecting Wireless LAN MAC Address Spoofing.” 01/21/2003. 05/27/2003 <http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf>

[9] Bird, Tina. “VPN Information on the World Wide Web.” 04/28/03. 05/27/03 <http://vpn.shmoo.com/>

[10] Phifer, Lisa. “Hot Spots Give Security Managers the Chills.” Information Security April 2003: Page 52.

[11] NetStumbler.com Downloads page, 05/27/2003 <http://www.netstumbler.com/download.php?op=viewdownload&cid=1&orderby=hitsD>

[12] AirSnort Homepage, 05/27/2003 <http://airsnort.shmoo.com>

[13] Kershaw, Mike. KISMET Documentation page, 05/27/2003 <http://www.kismetwireless.net/documentation.shtml>

Last Updated: October 24th, 2017

Upcoming Training

San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event