Wireless Security Attacks and Defenses

This paper provides great insight into properly securing Wireless LAN's. It's amazing the number of WiFi installations that are open to neighbors and others! Is your network as secure as it can be?

by Joshua Burke, Brad Hartselle, Brad Kneuven, and Bradley Morgan

Prologue

In office 411 on the fourth floor of the Herbert L. Smith Plaza, Diane Johnson, an accountant, was eagerly opening a package that had been delivered to her moments ago. She tore open the cardboard box and removed a shiny new 802.11g wireless router from the packaging. The instructions inside read clearly and were easily understandable, even by Diane who was a novice at best when it came to computers and networking. Within an hour she was connected to the company network using her personal laptop computer, which had come equipped with a factory-installed 802.11g antenna. Diane had recently seen a friend use wireless networking at their home and had decided to set up this wireless access point so that she could move about the office easily and still stay connected with the company network, as well as access her important accounting documents from her laptop. Diane was able to accomplish this without shelling out a lot of cash, and without having to learn a lot of networking jargon and skills. As she browsed the Internet in amazement of this intriguing technology, she convinced herself of her technological prowess and smirked at the haughtiness of the folks in her company's IT department.

Meanwhile, at the Cool Beans Coffee Shop across the street from the Herbert L. Smith Plaza sat a curious and devious individual. Taking a sip from his large double latte, he fired up his laptop computer and watched a myriad of startup command lines appear on his LCD in standard green and black monochrome. Using the antenna plugged into the PCMCIA slot of his computer and a collection of various open-source software programs, he began to scan the area for wireless networks. As the software began listing all of the detected access points in the range of his antenna, one in particular caught his attention. It was broadcasting itself with the name of "linksys" and it was determined by his software that the access point was broadcasting unencrypted data, or packets. From his experience, the man knew instantly that he was dealing with a wireless router that was using a factory configuration. With a few keystrokes, the man began to capture and examine the broadcasted packets from this transmitter, and with much amusement he scanned through numerous pieces of confidential accounting information that were originating from somewhere in the office building across the street.

A Brief Introduction to Security

Security - denial of access to assets for malicious intent. It is the capability to defend against intrusion and to ultimately protect your assets from access and disclosure, change, or destruction. A deeper interest within security is privacy, which is security of sensitive material for eye-only, often information about a person. In the corporate environment another form of privacy is encountered--material of a proprietary nature. This information is of particular importance to an organization because its disclosure could harm competitive advantage or divulge trade secrets.

Security takes three forms: physical, virtual, and data. We encounter physical security in our homes with locks; the same is true in industry. Physical security in the networking arena encompasses the protection of the physical assets, such as access points, wired channels, and the ultimate nodes. For the wireless domain, we don't think of physical security, we consider the next form, virtual security.

Virtual security is the ability to keep data secure when access is possible without physical access, i.e. access over a network. In wireless domains, this is a particular problem and is the subject of the rest of this paper.

Data security is generally the purpose and result of physical and virtual security, e.g., to deny an authorized persons access to data in transit or storage.

Wireless Security

Wireless technology can provide numerous benefits in the business world. By deploying wireless networks, customers, partners, and employees are given the freedom of mobility from within and from outside of the organization. This can help businesses to increase productivity and effectiveness, lower costs and increase scalability, improve relationships with business partners, and attract new customers. Indeed, there are numerous reasons to deploy wireless technology, but like most, it is not without its risks and downfalls.

The previous scenario illustrates just a few simple vulnerabilities that exist within the realm of wireless networking. We saw how confidential accounting data was compromised due to the actions of a well-intentioned employee with a simple lack of knowledge in what she was doing. It could have been much, much worse. Had our mysterious hacker been more proficient, he could have disabled critical software, initiated a denial-of-service attack, erased or destroyed data, or even wiped out the entire network, resulting in the complete stoppage of business functions.

While this may seem like a frightening outcome, there are many different ways to overcome the imperfections native to wireless networking. This paper is designed to help you understand these flaws and to assist you in making your wireless networks a secure and beneficial asset.

The State of the Wireless World

In June of 2004, WorldWide Wardrive 4[1] reported that an alarming 61.6 percent of all submitted wireless access points were broadcasting data with no encryption enabled. That is, the data (or packets) in being sent by their wireless hardware could be easily viewed by anyone listening in. This could include usernames, passwords, credit card numbers, or other sensitive information. The study also showed that 31.4 percent of the logged access points were using default SSIDs (which makes them easy to find and access) and that 27.5 percent were using no encryption with default SSIDs. The study found that the amount of access points using no encryption decreased by 6.04 percent from the previous year's endeavor. However, the number of wireless networks broadcasting default SSIDs and which used no encryption *and* default SSIDs actually increased by 3.57 percent and 2.54 percent, respectively. Even as time passes and awareness increases, there will always be more room for improvement in securing our airwaves.

As time goes by, improvements are being made in wireless standards, but it has yet to be seen whether or not wireless hardware in itself will eventually take care of security flaws. Contrary to beliefs in the IT profession, the recently released 802.11g standard does very little to improve upon the state of wireless network security. It should not be assumed that security problems will take care of themselves; we must familiarize ourselves with the vulnerabilities and the defenses of wireless networking in order to protect our businesses from the possibility of attacks.

What is 802.11?

In this text, when we are discussing wireless security we are referring to 802.11 networks. 802.11, or the Institute of Electrical and Electronic Engineers (IEEE) 802.11, which is a set of standards for radio communications used in wireless local area networks, or WLANs. IEEE is an organization composed of engineers, scientists and students that specialize in creating standards for the computer and electronics industry in order to ensure smooth operability and compatibility. The organization uses a number system to represent the standards it comes up with for different technologies. IEEE uses the number 802 to categorize standards for local and wide area networks, while the number 11 narrows that down to wireless area networks. In our discussions, you will also notice certain letters that appear after the number 11. These letters represent the different versions of the protocol, which specify things such as what frequency they operate in, and bandwidth they employ. These letters can also specify different security methods, as well.

802.11 networks are everywhere. The number of shipped 802.11-enabled hardware devices is estimated to exceed 40 million units by the year 2006 (Vladimirov, Gavrilenko, Mikhailovsky). Because of the popularity of this communications standard and its prevalence in the world of organizational wireless networking, our focus in this text will be primarily on 802.11 WLANs. By familiarizing yourself with the various aspects of the 802.11 standards, you will also be familiarizing yourself with the same technologies that are employed within the business world.

Vulnerabilities and Attack Methods

Human Error

It is understood that an individual with no understanding of networks can easily set up a flawed and vulnerable network. However, some executives need to be aware that even their system administrators could be lacking in their understanding of wireless network implementations. With the broad number of floating, corporate hotspots being found everyday it has be to be assumed that some of those hotspots were put into place by knowledgeable IT staff within those corporations. However, some of those techs missed something. Maybe a manager gave some of his development staff permission to install a wireless router while providing no oversight to the installation. Though developers may know something about software architecture and design, they may or may not know anything about network security. Perhaps the local system admin doesn't thoroughly understand networking principles. Maybe s/he lacks the tools necessary to carefully monitor network traffic and detect anomalies that could indicate the presence of a rogue access point[2]. Worst case, s/he might not even care. This can be extremely problematic in that network assets may be compromised, unbeknownst anyone in the organization. Your company should make sure that system administrators are well trained with a strong background in computer and network security.

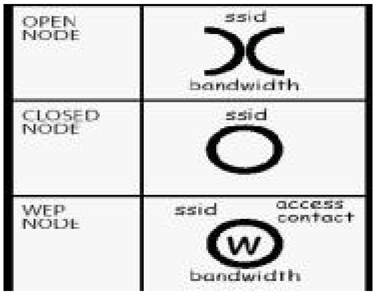
In any system, the human components are the weakest link. Wireless networking is certainly no exception. Your organization should define strict policies and procedures related to wireless networking within a well-publicized company document. It is especially important with regard to wireless networking that employees are made aware of these rules. As you saw in the opening vignette, an unwitting employee with good intentions compromised company data without even knowing she had done so. Because wireless hardware is cheap and relatively easy to use, the risk of your network containing rogue access points is great. You should be sure to set standards for any wireless hardware configurations within the company network and perform routine network audits to ensure that there are no open doors. We will discuss more specifics of wireless networking policies and procedures in our discussions on defense methods.

Rogue Access Points

As discussed earlier, it is easy for even a novice to acquire equipment and set up a wireless network. If this is done from within another network, it creates what is known as a subnet, which can create back doors to its parent. There are many easily overlooked mistakes that can be made in configuring a wireless network, many of which novice users will overlook. Individuals who wish to intrude upon a network can also plant rogue access points themselves. Network administrators must make sure to implement strict polices regarding the deployment of wireless hardware, and audit their networks often with reliable tools to ensure that these rogue access points do not exist.

Warchalking

Another point of interest before moving on is something, which is possibly more of a compelling idea than a physical reality called *warchalking*. It is a modern version of the hobo sign language used to alert one another to places providing shelter, food, and potential trouble. Using a fairly universal hobo sign language, individuals mark structures that have hotspots associated with them. In many cases these symbols incorporate much information about each node and the type of security currently being implemented. According to John Hiler, a New Yorker who writes about blog culture on his microcontent news site http://www.microcontentnew.com, warchalking is a "perfect storm" of three major tech themes. "It's got Wi-Fi. It's got the tie-in to hobo language, which is really cool from a linguistics point of view. And it ties into the spirit of democracy, which was the original intention of the Web," he said. "It's the subversive idea of giving the finger to the local land-line monopoly."



Common Warchalking Symbols and Terminology

MAC Address Spoofing[3]

Media Access Control (MAC) addresses [4] act as personal identification numbers for verifying the identity of authorized clients on wireless networks. However, existing encryption standards are not foolproof. A hacker can pick off authorized MAC addresses and steal bandwidth, corrupt or download files, and wreak havoc on an entire network. While securing your wireless LAN by using an authorized list of MAC addresses for authentication will provide some security, they were never intended to be used in this way.

There are a few legitimate reasons and examples of why you would want to spoof your MAC address:

- A firewall could be set up to only accept traffic from a certain MAC address at a certain time. An administrator could generate a list of MAC addresses that would change every certain number of days, hours, or even minutes. The user would have to set their MAC address within the time window to send packets to the firewall.
- Some ISP's keep track of the MAC address that a subscriber is using. They only allow registered addresses to connect to the Internet, and charge more money for additional IP clients. It might become inconvenient to be limited to a particular MAC address if a user needs to change the gateway or change cards in the gateway temporarily and would have to re-register a new MAC address just to move some equipment around for a few days.

Even if you are using encryption or virtual private networks (VPNs), MAC addresses are always in the air. With software such as *Kismet* or *Ethereal*, a hacker can capture the MAC address of an authorized user. They can then change their MAC address to the valid user's MAC address using any number of spoofing or cloning utilities, or even manually changing the Windows registry entry. Now the hacker can connect to the wireless LAN and bypass any MAC address filtering. *Netstumbler* can also be used with a MAC spoofing utility or MAC address modifying utility such as SMAC to achieve the same results.

Noisy Neighbors

The proximity of other wireless networks and equipment to that of your own is of utmost importance, for these can be a cause of or noise within your network. Because we are dealing with radio waves passing through the air, unwanted radio signals can wander into our domain from outside sources such as cordless phones, microwave ovens, or the neighboring business' 802.11 router. This noise, or interference can have a drastic effect on network performance and reliability.

Aside from the noise related issues, network users within an earshot of your access point could be consuming your bandwidth. Windows XP's built-in Wireless Zero Configuration utility, for example, is set up by default to join the wireless network with the best signal. Once it has successfully connected, it stores the network SSID as a "preferred network" and will connect to it each time it comes within range. Though this is convenient in most circumstances for the network client, it can lead to unwanted network users. Even with WEP enabled, which can keep unwanted clients from joining your network; would-be clients knocking on the door, requesting connections, can consume significant bandwidth. Auditing and scanning your network, methods of which we will discuss later, can minimize noise from and overlapping of neighbor networks.

Caveat: Interference of this type was recently experienced at a conference in Las Vegas, Nevada. Attendees were invited to connect to the conference's wireless network at a designated hotspot within the venue. One attendee in particular attempted to connect to the advertised access point for ten minutes before giving up and venturing to a nearby *Starbucks* coffee house where he paid $9.95 for a day's access to *T-Mobile*. The problem at the conference center was due to two problems. First, there were some 35 active access points in the large display room, all using the same 802.11b/g frequencies and, thus, causing both interference and using overall bandwidth. Secondly, the little bandwidth that was left was being shared by dozens of users of these public access points.

Improper Design

Improper or unknown boundary definitions constitute another possibility for network design error. Wireless network interface cards (NIC) and routers come with a variety of antennas. Some antennas broadcast in a single direction, and while they are not very accommodating to the surrounding area, they definitely help narrow the boundaries. The real danger comes in omni-directional antennas that broadcast in all directions, providing easy-access to the wireless network. Below is an illustration giving an example of improper boundary definition for a wireless network.

Caveat: Both of these antenna installations are omni-directional. The one on the left is confined to a single floor and does not broadcast beyond the walls. The one the right, however, does both.

Notice how the second example in the illustration shows the access boundary of the wireless network extending outside the corporate structure in which the network has been implemented.

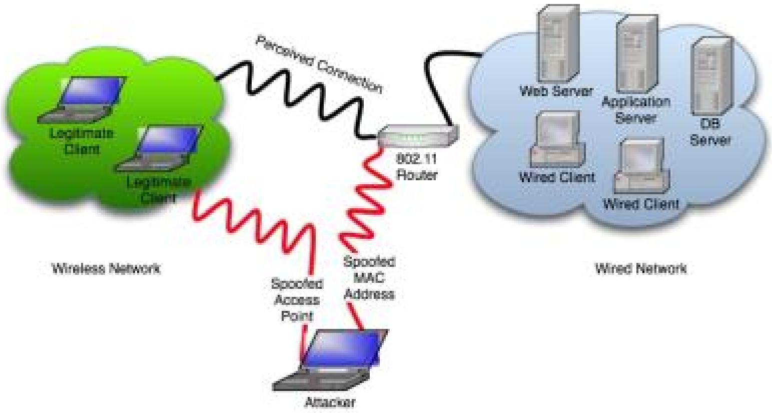
Insecure-by-default hardware, unqualified system administrators and coverage boundaries that are out of control make up the key characteristics of faulty wireless network design.

Man-In-The-Middle Attacks

Hailing from the early days of cryptography, man-in-the-middle attacks are an old strategy applied to a new technology.[5] The key concept behind a MITM attack is exactly as it sounds, one entity with malicious intent intercepts a message between two communicating entities. The hijacker can then send the message onto the receiver as if it had never been delayed, and even alter the message's content. Used in war, this could be a valuable tool for intercepting and altering the enemy's message to suit the opposing side's purposes. In World War II, if the Axis forces needed to send information to deployed troops, they would send it with a decryption key. This key would be the primary tool for decoding the message and properly deciphering it. If the Allies could intercept this message and break the code, then they would be executing a MITM attack. Upon successful completion of the attack, they'd have three options as to how they'd like to exploit the position.

- The message could be intercepted, altered and sent onto the recipient with fraudulent information.
- The message could be blocked and prevented from proceeding any further.
- The message could simply be read and sent on its way without the recipient's knowledge.

The concept for MITM attacks on wireless networks is the same.



A Diagram Depicting the Anatomy of a Man-In-The-Middle Attack

The method of attack is simple in application, provided you have the right kind of software. Fortunately for a hacker (unfortunate for a director in charge of security), there are several applications available as freeware that perform the tasks necessary to execute a proper MITM attack.

The first task associated with an MITM attack comes into play after the initial tasks for hacking a wireless network have been performed. That is to say, we are assuming that a target network has been located, and that the attacker is within acceptable range of a target access point. Once these tasks have been performed the MITM process can begin.

After having captured information about the target access point, a "soft AP" can be set up by placing a WLAN card on the attacker's machine into host mode with the same, or similar, properties as the legitimate access point. This soft AP can then attract clients who think they are connecting to a familiar network. At such a time, the attacker can use another WLAN card to forward the traffic to the real access point, all the while capturing any information that moves across its path.

In some access controlled networks, all hosts on a network store a list of acceptable MAC addresses for their respective network. Using the ARP method, those systems can validate IP addresses that request access to their network by resolving them against a known table of valid IP/MAC addresses. MITM can thwart this defense by piggybacking on another attack method called ARP Spoofing. Many systems easily accept ARP commands and freely allow their MAC lists to be updated. Using software like ARPoison[6], an attacker can add their own MAC address to the list or trick the system into sending that table to the hijacker's system. ARPoison uses the ARP Spoofing to trick the network into sending all of their ARP requests to the hijacker's system instead of a valid host. Once the request comes in, the hijacker can reroute the information to a valid host, but only after they have had extensive access to the transaction. Once the attacker has established themselves as valid members of the network they can:[7]

- Execute a denial of service(DoS)[8] by sending all host requests to invalid host addresses, thus causing bounce backs.
- Monitor all transactions between the hosts (hence "Man-In-The-Middle").
- Join the network by adding the attacker's MAC address to the acceptable list.

There are many other types of software applications that can perform these ARP poisoning methods, as well as execute other hacking techniques such as port sniffing. By utilizing Level two layer vulnerabilities through ARP Spoofing, MITM techniques are easy to execute, and expensive to detect.

Basic Defense

WEP

Wireless Encryption Protocol was integrated into wireless devices with a primary goal of preventing casual eavesdropping on a network. Much like crosstalk can occur among wireless telephones, the same effect could take place in getting packets distorted among common pathways on a wireless network. WEP performs this function rather well, but the second purpose of WEP is where the protocol falls short. The second purpose of WEP is to prevent unauthorized access to wireless networks. Now don't be mistaken, WEP will prevent uninformed and unskilled crackers from accessing a wireless network. However, it doesn't take much effort at all to break WEP. While the methods of attack that can be used are too technical for our purposes, it's important to understand their existence.

One method comes in the form of brute force attacks, which simply break down WEP's functionality forcing errors within the protocol and eventually causing it to open a door on its own. Other algorithms exist such as the dictionary attack. Dictionary attacks use several common keys, or a dictionary of keys stored over time to try guessing a different key until one works. Deeper hacking methods involve exploiting what is called the IV (Initialization Vector) vulnerability. The Initialization Vector can be used to trick WEP systems, and manipulate them into revealing keys or simply breaking down defenses by causing confusion within the WEP transmissions.

A few improvements have been attempted in regards to WEP mainly in the form of WEP2. WEP2's primary attempt at improvement came in making the IV key even longer. However, industry experts agree that this not only doesn't make WEP more secure, but also exposes even greater security threats to users.

WEP does a fine job at keeping novice hackers from spying on your valuable data. However, armed with the right tools, WEP has been proven to be flawed and vulnerable. We recommend that network administrators make use of WEP but emphasize that primary dependence not be placed on this protocol for security. WEP should be used, even according to wireless product makers like Netgear, but certainly not by itself.

Even with its inherent weaknesses, Wireless Encryption Protocols or WEP is still a good method for preventing attackers from capturing your network traffic. Less-experienced hackers will probably not even attempt to capture data packets from a wireless network that is broadcasting using WEP. Even if a hacker possesses the skills and tools necessary to crack WEP, it can be an extremely time-consuming process, especially when dealing with the newer 128-bit specification, which requires in excess of 500,000 captured data packets to even begin the cracking process. Not only is WEP a good way to ward off many would-be attackers, it is strengthened when used with other security techniques.

MAC Address Blocking

For smaller, more static networks you can specify which computers should be able access to your wireless access points. Telling the access points which hardware MAC addresses can join the network does this. Although, like WEP, in which this can be bypassed by knowledgeable hackers, it is still a valid method for keeping many intruders at bay.

Ditch the Defaults

Most wireless devices are being sold today with default configurations that are easily exploited. The three main areas to watch out for are the router administration passwords, SSID broadcasting, and the channel used to broadcast the signal. Upon installation many users would do well to immediately change the router's administration password. The default passwords are easy to locate provided you can gain access to the user's manual associated with each device. Turning off the SSID broadcast option will prevent unintentional wireless hijacking because rogue wireless devices will not be able to automatically detect the SSID without extra action. Changing the default-broadcasting channel will also make a WLAN more unique in its architecture and thus less difficult to detect based on default vulnerabilities.

Beacon Intervals

Another AP configuration that is recommended being changed is the beaconing interval. The beaconing interval is a frame that is sent out to announce the presence of the AP. Client stations use this to configure parameters to join a network. This is a separate from the SSID broadcast in that a beacon frame appears as a random data packet without a SSID label. These intervals should be maximized to make it more difficult to find the network.[9] The network appears quieter and any passive listening devices are not as productive at gathering and cracking encryption keys.

Access Lists

Using MAC ACL's (MAC Address Access List) creates another level of difficulty to hacking a network. A MAC ACL is created and distributed to AP so that only authorized NIC's can connect to the network. While MAC address spoofing is a proven means to hacking a network this can be used in conjunction with additional security measures to increase the level of complexity of the network security decreasing the chance of a breach.

Controlling Reset

Something as simple as controlling the reset function can add a great deal of security and reduce the risk of potential hack to your network. After all the security measures are in place and the proper encryption settings are enforced, the factory built "reset" button available on nearly all wireless routers/AP's can, in an obvious way, wipe out everything.

Disable DHCP

Disabling the use of DHCP in a wireless network is again, a simple but effective roadblock to potential hackers. In the event that a threat breaks through your encryption they would then have immediate access to the network if they were assigned an IP address by DHCP. This may not be feasible in a large corporate environment where thousands of IP addresses are leased throughout the day, but in a home space this is a must for all users.

Network Auditing and Intrusion Detection

Network administrators should equip themselves with the proper tools for auditing and troubleshooting their wireless networks. However, one of the tricky things about detecting intrusions on a Wireless LAN is the amount of time and resources that must be committed to monitoring the network. The kinds of tools available range from simple software solutions, to complex hardware devices. Depending on the size and sensitivity of your network (and your budget) these tools can range from completely free to extremely expensive.

Two leading technologies that are gaining momentum in enterprise and small business LANs alike, are IPS, and IDS. Intrusion Prevention Systems try to take a proactive measure in network security, so as to stop the attack before it starts. Intrusion Detection Systems are more passive in their methodology, monitoring and informing network administrators of any intrusive presence.[10] Both of these systems monitor networks, whether they are WLANs or LANS, over extended periods of time. This frees up network administrators to perform other tasks associated with network management until they are made aware of a need for action. Douglas Conrich, IBM's Global Solutions Manager, calls these kinds of attacks, ‘Texas barbeques'.[11]

Today's IDS/IPS systems can be employed in many different ways. According to some research analysts' there are three different ways to employ this technology. The first method involves a software solution that simply uses the existing access points on the network to keep an electronic eye on traffic patterns. This method suits the needs of many smaller businesses that don't have the expertise or budgets to go any further. The second method is by using what are called passive 802.11 monitors that watch over any and all wireless activities in the area. All the data recorded by the sensors are sent to one central server for processing and analysis. This provides a much more comprehensive view of wireless activity, as well as adds the capability of detecting rogue access points that would go on unbeknownst in the first method. There is also a third method which places more of the processing load on the sensors themselves. In this case, the sensors don't report back to the central server unless they discover something suspicious.[12] In either of the last two methods, once the anomalies have been reported to the central server, employees can be deployed onto the premises to track the source of the intrusion. One advantage in WLAN security is that in most cases the intrusion has to be local, whereas in a wired attack, the attacker could be on the other side of the world.

An interesting observation made by many experts, is that most companies that are interested in IDS/IPS technologies want them to enforce a zero wireless policy. Some corporations would rather just eliminate the possibility of wireless technology on their network all together. The reasoning behind this lies in the very real threat of using wireless attacks to invade wired networks.[13] Being able to setup an ad-hoc wireless access point allows someone too intentionally or unintentionally connects to the wired network and then disconnect, making the intrusion very difficult to trace.

A wide variety of tools are available to survey your wireless domain, many of which we detailed earlier in this paper. They can do such things as measure the distance of your AP signal and control power output if it extends beyond the limits of your premises, or alerts you to suspicious activity on the network.

Surveying your own network can also be looked at as just trying to hack your own setup. What better way to test your security than to run one of the wireless hacking tools against your security? Many of the tools freely available to crack a wireless network are simple enough that most intermediate windows users could begin their own war chalking movement.

There are also a limited number of software tools available that allow you to deploy wireless Intrusion Detection Systems or IDS, which can automatically monitor the network and report suspicious events that occur to system administrators. These suspicious events can include things such as the presence of unusual data packets, the presence of new wireless transmitters in the area, or traffic encrypted with unknown WEP keys. The following table details several of the commercial and open-source wireless LAN auditing tools available for use today.

Commercial	**Open Source**
AirDefense: Uses devices called IDS sensors which are placed around the network and report information to a central management server or console	WIDZ: Offers rogue AP detection and monitors the network for possibly hostile traffic
WiSentry: An entirely software based IDS which distributes a small client process to detect suspicious activity	AirIDS: Offers basic IDS capabilties
AirMagnet: Offers a suite of software tools used to diagnose security issues and other wireless network problems	Kismet: Can detect suspicious hosts such as clients running AirJack and dictionary attacks
NAI Sniffer: A wireless protocol analyzer with IDS functionality	HotSpot-Defence Kit: Monitors the WMAC address, ESSID, and various other indicators that have been picked up by a rouge AP like sudden fluctuations in signal strength. This application was released in part by the overwhelming demand for something that would prevent the attack, as hacker tools like AirSnarf become increasingly easier to get and use.
AiroPeek – A wireless protocol analyzer with IDS sensor functionality	

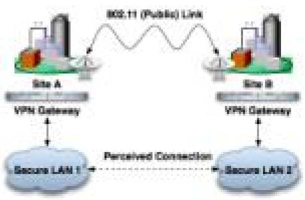
Virtual Private Networks

Virtual Private Networks, or VPNs, facilitate security over public connections through encryption techniques and other various security methods. A VPN works by sending data through a "tunnel" which cannot be penetrated by paths outside of the tunnel. This is done through the use of tunneling protocols such as Layer Two Tunneling Protocol, which encrypts the data at the sending end, and decrypts it at the receiving end. In order for a VPN to function properly, network users must install a small client application on their computers, which is used to decipher and help facilitate the encoded communication.

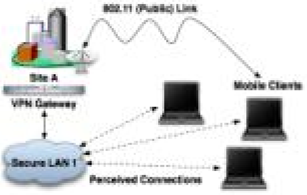
A protocol called IPSec is the de facto standard for VPN's over the Internet. IPSec defines the way secure data packets are structured through its three major components: the Authentication Header (AH), the Encapsulating Security Payload (ESP), and Internet Key Exchange. AH is responsible for verifying that packets have not been altered between the sender and receiver. It does not provide any encryption—it simply verifies that the data sent through a VPN is accurate. Encryption is handled instead by ESP, which can employ a variety of techniques such as Data Encryption Standard (DES) or Secure Hashing Algorithm (SHA). Each of the three components can operate in different modes and can be combined in different ways, which allows customizable security through implementation. For example, many IPSec VPNs either do not use AH at all, or use a combination of AH and ESP.

Common VPN Protocols	
IPSec	IP Security - The most widely acknowledged and used of the protocols, which uses an open-standard framework for interoperability.
PPTP	Point-to-Point Tunneling Protocol - A Microsoft developed protocol that is used mostly for secure communications channels between a large number of Windows hosts.
GRE	Generic Routing Encapsulation - A Cisco developed protocol that does not provide encryption by itself, but is used with other protocols to secure communications channels.
L2TP	Layer Two Tunneling Protocol – Developed jointly by Cisco, Microsoft, and 3Com. This protocol was created to replace PTPP as a major tunneling protocol, and like GRE, does not offer encryption by itself.

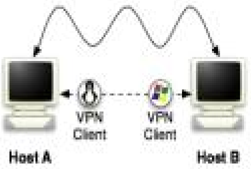
VPNs fit into three categories: network-to-network, host-to-network, and host-to-host. Network-to-network VPNs are used to securely transmit data between two LANs over a public network. Host-to-network VPNs connect a single user to a LAN securely, over a public network. Finally, host-to-host VPNs involve two single clients communicating securely with one another over a public network.



Network-to-Network VPN



Host-to-Network VPN



Host-to-Host VPN

The main advantage of VPNs is that they are a cost-effective way of connecting remote nodes or sites. Alternatives to VPNs, such as dedicated, leased lines or deployment of a Remote Access Server are much more expensive. As a matter of fact, a free VPN solution called FreeS\WAN exists for Linux systems.

Home Grown or Advanced Encryption

Another advanced defense method that is possible, although unlikely, is to create an in-house encryption algorithm to use for encoding your network's data. Not only would you need some very sensitive data to justify this, but you would also need highly skilled, technical staff. Also, be advised that by implementing self-made encryption techniques, you could create a very strong, unknown encryption scheme, which works extremely well, or you could possibly create one that is easily crackable or flawed.

A more likely approach would be to implement an existing, proven encryption method such as MD5 or MIC. Many different encryption techniques exist and information on how they work and how to implement them is freely available in books or online. Should you choose to go this route, make sure you have a skilled staff on hand to handle the project.

The intricacies of encryption are outside the scope of this paper. Our purpose is to merely point out that the above options exists as a method of defense in the arena of wireless security.

Summary

We have taken a look into many facets of 802.11 WLANS. We have seen their benefits and risks, their strengths and weaknesses, and we have learned some ways in which they are attacked and defended. As wireless technology continues to expand its presence across the globe, there are sure to be many fascinating changes that will affect the way we live and work--and it will be important to have an understanding of the both the possibilities and dangers that come with it. Without a doubt, there will be improvements made to wireless security. Along with that will come new methods of attack and defense, as well as many other changing characteristics. We hope that the knowledge contained in these pages provides a solid understanding of wireless security, and a foundation on which to build and adapt knowledge as changes come about.

References

1. Boscia and Shaw, "NASA Advanced Supercomputing Division: Wireless Firewall Gateway White Paper", http://www.nas.nasa.gov/Groups/Networks/Projects/Wireless/, September 3, 2004.
2. Cisco Systems, Inc. "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite", http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf, 2002.
3. The Honeynet Project, "Know Your Enemy: Sebek", http://www.securitydocs.com/library/2769, December 10, 2004.
4. Karygiannis and Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices", http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
5. Vladimirov, Gavrilenko, Mikhailovsky. Wi-Foo: The Secrets of Wireless Hacking. Boston: Addison-Wesley, 2004
6. WarDriving, http://www.worldwidewardrive.org
7. Webopedia, http://www.webopedia.com
8. "Wireless Security Recommendations for Rutgers", http://techdir.rutgers.edu/wireless.html, November 3, 2003.

[1] The WorldWide WarDrive is an effort by security professionals and hobbyists to generate awareness of the need by individual users and companies to secure their access points. The goal of the WorldWide WarDrive (or WWWD) is to provide a statistical analysis of the many access points that are currently deployed. See http://www.worldwidewardrive.org for more information.

[2] Rogue Access Points are entry points into a WLAN that can be either intentionally or unintentionally placed on the WLAN.

[3] Spoofing - To fool. In networking, the term is used to describe a variety of ways in which hardware and software can be fooled. *IP spoofing*, for example, involves trickery that makes a message appear as if it came from an authorized IP address. (www.webopedia.com)

[4] ***Media Access Control address***, hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sublayers: the *Logical Link Control (LLC) layer* and the *Media Access Control (MAC) layer*. The MAC layer interfaces directly with the network medium. Consequently, each different type of network medium requires a different MAC layer. (www.webopedia.com)

[5]In cryptography, a **man in the middle attack** (**MITM**) is an attack in which an attacker is able to read, and modify at will, messages between two parties without either party knowing that the link between them has been compromised. (www.webopedia.com)

[6] ARPoison, http://web.syr.edu/~sabuer/arpoison/, (accessed October 2004)

[7] Wagner, Robert, "Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks", SANS Institute
www.sans.org/rr/papers/60/474.pdf, accessed Oct 2004.

[8] http://www.webopedia.com/TERM/D/DoS_attack.html - Short for ***denial-of-service** attack*, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

[9] Karygiannis and Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices", http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf , November 2002.

[10] Lisa Phifer, "WIDS Overview: Helping Customers Spot Wireless Intruders", http://isp-planet.com/fixed_wireless/technology/2003/wids_overview1.html, October 14, 2003.

[11] Lisa Phifer, "WIDS Overview: Helping Customers Spot Wireless Intruders", http://isp-planet.com/fixed_wireless/technology/2003/wids_overview1.html, October 14, 2003.

[12] Gabriel Brown, "Wireless IDS Is All the Rage", http://www.unstrung.com/document.asp?doc_id=42313, October 22, 2003.

[13] Mia Shopis, "Wireless IDS, a crucial part of your security strategy", http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci931628,00.html, October 10, 2003.

[14] Diagrams by Bradley Morgan