What You Will Learn

By the end of this chapter, you should know and be able to explain the following:

- ✔ The essentials of wireless LANs, including their benefits and risks
- ✔ The major threats to a wireless network
- ✔ The breadth and scope of possible attacks and exploits that are available to attackers

Being able to answer these key questions will allow you to understand the overall characteristics and importance of network security. By the time you finish this book, you will have a solid appreciation for network security, its issues, how it works, and why it is important.

CHAPTER 8

Wireless Security

> *In the end, we will remember not the words of our enemies, but the silence of our friends.*—Martin Luther King Jr. (1929-1968)

When was the last time you went on vacation to get away from it all? Perhaps to some remote beach or maybe a getaway to the country? Imagine that you walk out the patio door of your hotel room (an ocean view, of course) and admire the beauty of the sun setting on the ocean. The air is cool, so you decide to sit on the porch in your favorite lounge chair; the sea-gulls are playing, the waves are breaking in a rhythmic beat, and *beep-beep-beep*—your pager begins to go off!

Who could possibly be paging you while you are trying to relax and unplug? What emergency could be so grave that it would require you to be interrupted on this fantasy vacation?

According to the message on the display, there seems to be a problem with the company firewall/VPN/Exchange server/<insert emergency here>. It looks pretty serious, so you conclude that you need to log into your office network and take a look.

It is a good thing that you chose a hotel with high-speed Internet access, and that you brought your wireless access point. The access point is plugged into the high-speed LAN port via wireless so you can still enjoy the beautiful view. You cannot really avoid turning on the laptop that you were not planning to turn on while you were on vacation; you are needed for an emergency.

So, here you are on the patio booting up your laptop. You see the "blinky-blinky" of the wireless NIC's status lights. All systems are go!

You fire up Telnet and proceed to log in to the router/firewall and start snooping around to see what the problem could be. This should not take too long, you say to yourself. There is still plenty of time to enjoy the rest of the evening and perhaps have a nice dinner. An hour goes by and you have solved the problem. You are quite taken with yourself for being ingenious enough to diagnose and resolve the situation within a few tick-tocks.

Screeeech…stop the movie for a second. Unknowingly, the "vacationing uber tech" just caused his company to lose millions of dollars. How, you might ask, did this guy in the movie cause millions of dollars to be lost just by logging in to his company's router/firewall to fix a problem?

It was not the act of telnetting to the router/firewall that caused the problem; it was the fact that he used a wireless connection. You see, the company that uber tech worked for (yes, past tense cause he no longer works for them as a result) is a multinational corporation that was about to announce the creation of a new widget that was capable of converting discarded pizza boxes into SDRAM memory chips; a competitor of this revolutionary company not only wanted to stop this announcement—but they also wanted a copy of the plans for this widget so they could bring it to market first.

It seems that a hacker employed by the competitor was paid to follow vacationing uber tech and, at a convenient moment, break into his hotel room and download the contents of his laptop to a portable storage device, in hopes that the hacker could find some proprietary information about the widget. Upon seeing uber tech boot up his laptop, complete with wireless NIC, the hacker realized that he had struck gold and decided to do some long distance sniffing and hacking, courtesy of uber tech's unsecured wireless connection. Long-distance sniffing and hacking—sounds like a script from "Mission Impossible," doesn't it? Too far fetched to really happen? The truth is that this type of scenario occurs on a daily basis. Bad guys with wireless-enabled laptops steal information right out of the air with little effort. They use tools that are readily available on the Internet and can cause many problems for companies that do not take the time to understand the threats an unsecured wireless connection poses to their corporate network.

This chapter covers several topics related to wireless networking security and helps you identify, understand, and prevent the types of intrusions to which wireless connections are vulnerable from the outside. This chapter focuses on the commercial wireless products that are available and not the home version from Cisco subsidiaries such as Linksys. It is important to understand the differences; in this article describing the Cisco Linksys acquisition, there is a clear, related message:

> Take, for example, Cisco's Aironet wireless products. The Aironet products are the result of Cisco's significant investment in industry-leading WLAN and networking technology. Cisco Aironet solutions offer premium value in security, range, management, performance, features, and total cost of ownership as part of a complete, complex network. Linksys' products, on the other-hand, are developed using off-the-shelf silicon and software and focus on ease-of-use, price, and features that are important to consumers. As you can see by this example, the products are geared towards a different market with different needs.
>
> http://newsroom.cisco.com/dlls/hd_032003.html

Essentials First: Wireless LANs

This chapter discusses the use of Wireless LANs (WLANs), which are roaring into use almost every time you turn around—from airports, restaurants, and coffee shops, to people's homes. The growth of personal computers in the 1980s led to the creation of LANs and the Internet in the 1990s; this allowed for connections, regardless of geographic location. WLANs are proving to be the next technology growth area for the 2000s. Businesses are, of course, recognizing the benefits of WLANs and deploying them in ever-increasing numbers. Just as businesses were forced to provide security to PCs and the Internet, so too must businesses understand that, despite the productivity and mobility gains they provide, WLANs have associated security risks that must be addressed.

WLANs offer a quick and effective extension of a wired LAN. By simply installing access points to the wired network, personal computers and laptops equipped with wireless LAN cards can connect with the wired network at broadband speeds (or greater) from up to 300 yards away from the wireless access point. This means that computers are no longer tied to the infrastructure of wires—rather liberating, isn't it?

The majority of WLAN deployments have used a wireless transmission standard known as 802.11b. The IEEE 802.11b standard operates at the radio frequency of 2.4 Ghz—a frequency that is unregulated by governments. The 802.11b standard offers connectivity speeds of up to 11 Mbps, which provides enough speed to handle large e-mail attachments and run bandwidth-intensive applications like video conferencing. While the ***802.11b*** standard now dominates the wireless LAN market, other variations of the 802.11 standard are being developed, or have already been approved, to handle increased speeds. ***802.11g*** is the latest standard variation, which offers wireless speeds of up to 56 Mbps.

The various wireless standards are targeted to different industry segments as outlined in Tables 8-1 and 8-2.

Table 8-1 802.11a/WLAN Standard Characteristics

Standard	IEEE 802.11a, WLAN
Frequency wavelength	5 GHz
Data bandwidth	54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 12 Mbps, 6 Mbps
Security measures	WEP, OFDM
Optimum operating range	150 ft. indoors, 300 ft. outdoors
Best suited for a specific purpose or device type	Roaming laptops in home or business; computers when wiring is inconvenient

802.11a never took off; however, the recently ratified 802.11g holds some interesting options to include increased speed and security as Table 8-2 documents.

Table 8-2 802.11g/Wi-Fi Standard Characteristics

Standard	IEEE 802.11g, Wi-Fi
Frequency wavelength	2.4 GHz
Data bandwidth	54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 12 Mbps, 6 Mbps
Security measures	WEP, OFDM, AES (in Broadcom 54 g) and possibly WPA/Wi-Fi protected access
Optimum operating range	1000 ft. under ideal conditions; expect more like 150 ft. indoors and 300 ft. outdoors under normal conditions
Best suited for a specific purpose or device type	Roaming laptops in home or business; computers when wiring is inconvenient

Note that when 802.11b clients are granted access to an 802.11g wireless access point, security inevitably must be set (lowered) to allow 802.11b clients on; thanks to WEP and its problems, the entire network is reduced to a lowest common denominator.

What Is Wi-Fi?

The term ***Wi-Fi (Wireless Fidelity)*** is often used in discussions of 802.11 networks. Wi-Fi is most certainly the popular marketing word used today when talking about wireless (that is, Wi-Fi hot spots). The term Wi-Fi is fast becoming the common way to describe 802.11 wireless networks; it certainly is much quicker and easier to say, so we let marketing take the credit for making it the mainstream term.

Wi-Fi also refers to certification by the Wi-Fi Alliance, an international nonprofit association of 802.11 product vendors. 802.11 products that receive Wi-Fi certifi-

cation have been tested and found to be interoperable with other certified products. This means that you can use your Wi-Fi certified product with 802.11 Wi-Fi certified networks, whether they are Apple Computers or Windows-based networks. Although 802.11 products that do not have Wi-Fi certification might work fine with certified devices, the Wi-Fi Certified logo is your assurance of interoperability. You can learn more about the Wi-Fi alliance online at: http://www.weca.net/.

Benefits of Wireless LANs

I had not flown much on airplanes recently, but an important family event—my brother's wedding—allowed me the opportunity to fly. Not living near a major airport meant that I had to connect to reach my destination, so I experienced four different airports, each of which offered wireless connectivity to travelers, making layovers in airports a more productive time. Businesses all across the world are using this wireless capability and can easily be enabled for a relatively small financial investment. The benefits of deploying wireless LANs can be summarized as the following:

- **Attractive price**—Deploying a wireless LAN can be cheaper than a wired LAN because you do not have the need for wires; simply hook up an access point, and it can provide service to multiple computers.
- **Mobility**—Boost user productivity with the convenience of allowing them to wirelessly connect to the network from any point within range of an access point.
- **Rapid and flexible deployment**—Quickly extend a wired network with the ease of attaching an access point to a high-speed network connection.
- **Application agnostic**—As an extension of the wired network, WLANs work with all existing applications. As discussed previously, the standard protocol is TCP/IP, which is supported over all forms of wireless.
- **Performance**—WLANs offer a high-speed connection that, while equal to Ethernet, is quickly passing it in speed.

The benefits of WLANs are being recognized by individuals and businesses alike; recently the Gartner Group predicted that by 2005, 50 percent of the Fortune 1000 companies will have extensively deployed wireless networks, and that by 2010, the majority of Fortune 2000 companies will depend on wireless technology to meet their business and networking needs.

Wireless Equals Radio Frequency

The first technical concept you need to grasp when discussing what constitutes a threat to a wireless network is that 802.11 networks use radio frequencies to transmit the data back and forth between endpoints, just like the cordless phones or radios you have at home. The key difference is the frequency at which the signals are transmitted.

Radio waves can travel long distances, depending on the frequency being used. Some frequencies can transmit 300–400 feet, requiring little power to do so. Most older technology cordless phones and wireless NICs use the 900-MHz frequency as a carrier wave, which can travel quite a bit farther than most people realize. It is not uncommon for a 900-MHz cordless phone to give a user at least one or two city blocks of use before the handset loses its connection to the base unit. One or two city blocks translates roughly to 400–500 feet.

If your telephone handset can transmit out as far as 500 feet, it means that your wireless connection is capable of similar distances. If you have a Wireless access point (WAP) installed in your office or home, you can bet that people walking by outside are well within its operational envelope. The same holds true if you have a WAP installed in your small office, home office (SOHO) network. If an average WAP is installed in your living room and you live in an apartment complex, you might already be providing Internet service to most of the complex and not even realize it.

Wireless Networking

The term ***wireless networking*** refers to radio technology that enables two or more computers to communicate using standard network protocols such as IP, but without cables. Wireless networking hardware requires the use of underlying technology that deals with radio frequencies and data transmission. The most widely used standard is 802.11, which produced by the Institute of Electrical and Electronic Engineers (IEEE). This is a standard defining all aspects of Radio Frequency Wireless networking.

802.11b specifies that radios talk on the unlicensed 2.4GHz band at 11-Mbps transmission rate on one of 15 specific channels (in the United States, use is limited to only the first 11 of those 15 channels because of government regulations). Wireless network cards automatically search through these channels to find WLANs, so there is no need to configure client stations to specific channels. When the NIC finds the correct channel, it begins talking to the access point. As long as all the security settings on the client and AP match, communications across the AP can begin, and the user can participate as part of the network.

note

802.11g is a new high-speed wireless standard that allows users to transmit data at rates of up to 54 Mbps—nearly five times faster than 802.11b technology. Because it operates in the 2.4GHz frequency band, 802.11g is completely compatible with 802.11b and available for use worldwide. Apple currently has support for 802.11g in all its devices, with Cisco to follow shortly.

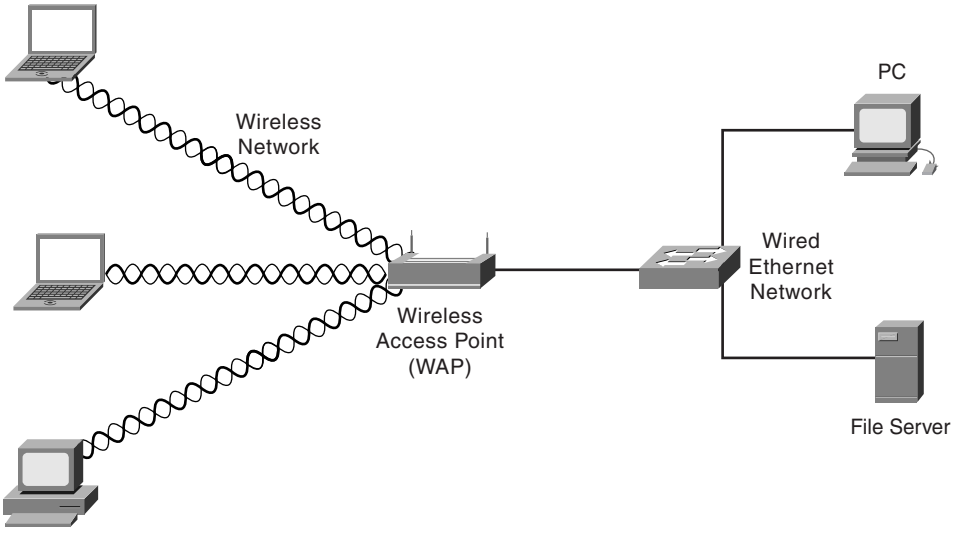
Modes of Operation

Two types of wireless networks are possible, and they differ on how wireless devices communicate to each other. WLANs operate either in ad-hoc or infrastructure. Ad-hoc networks have multiple wireless clients talking to each other as wireless peers to share data among themselves without the aid of a wireless access point. An infrastructure WLAN consists of several clients talking to a central

device called an access point (AP), which is usually connected to a wired network like a corporate or home LAN:

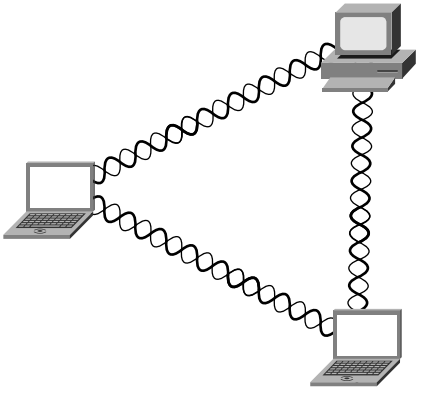
- ***Infrastructure*** — This mode of operation requires the use of a Basic Service Set (BSS); in other words, a wireless access point. The access point is required to allow for wireless computers to connect not only to each other but also to a wired network, as shown in Figure 8-1. Most corporate WLANs operate in Infrastructure mode because they require access to the wired LAN to use services such as printers and file servers.

Figure 8-1 Infrastructure Wireless Networking



- ***Ad-Hoc*** — Ad-hoc is also known as peer-to-peer wireless networking, as shown in Figure 8-2, where there are a number of wireless computers that need to transmit files to each other. This mode of operation is known as Independent Basic Service Set (IBSS). You can think of ad-hoc as being able to happen without the use of an access point. Each computer can communicate directly with all the other wireless enabled computers. They can share files and printers this way but are *unable to access wired LAN resources* unless one of the computers acts as a bridge to the wired LAN using special software. (This is called bridging.)

Figure 8-2 Ad-Hoc Wireless Networking



Coverage

Entirely too many wireless access points are available these days to cover them all, so this section focuses on the general coverage levels available. Your mileage might vary, so always check with your manufacturer and do a little WarWalking to see what is happening.

Every wireless access point has a finite range within which a wireless connection can be maintained between the client computer and the access point. The actual distance varies depending on the environment; manufacturers typically state both indoor and outdoor ranges to give a reasonable indication of reliable performance. Also, note that when operating at the edge of the range limits, the performance might drop because of deterioration of the quality of the wireless signal. Typical ranges are as follows:

- Typical indoor ranges are 150–300 feet but can be shorter if the building construction interferes with radio transmissions. Longer ranges are possible, but performance degrades with distance.
- Outdoor ranges are quoted up to 1000 feet, but again, this depends on the location and the environment.

In most cases, separate access points are interconnected via a wired LAN by providing wireless connectivity in specific areas such as offices or classrooms. Depending on the sophistication of the access point, the range can be modified by adjusting the power level on the AP. This might or might not be an option on some of the lower-end consumer level APs; however, on the Cisco Aironet 350, 1100, and 1200 series, this is possible. The ranges are 5 mw to 100 mw, which can be a useful method of controlling how far your signal reaches outside your company walls.

If a single area is too large to be covered by a single access point, multiple access points or wireless bridges can be used. If you choose to go this route, make sure that the access points you want to use have this feature because some do not.

Bandwidth Availability

Bandwidth on an 802.11b network is limited to 11 Mbps per access point. To dispel a lot of confusion, 11 Mbps refers to the *total possible bandwidth* per access point. Many people are used to the wired world, where switches are everywhere and each device gets the full 100 Mbps to the desktop. This is not the case with wireless; the 11 Mbps is divided among all users on that access point. If ten people access the same AP, communication to the wired world will be limited to the equivalent of approximately 1 Mbps per user.

So, you can solve the problem by simply adding another access point? I have not used the "it depends rule" since Chapter 4, "Security Protocols," so its use is way overdue and I am invoking it now. It depends; the 802.11b standard does not contain any specifications for load balancing across multiple access points. Devices that strictly adhere to the standard have no solution to the problem of finding your network becoming overpopulated.

The only way to manage this issue is to add another AP in the same area with a different network name and radio channel, effectively having more than one separate network with a maximum of three in use at the same area. Again, this is if you are using devices that adhere in this regard to the 802.11 standard. In reality, many manufacturers recognized that they would be severely limited in the number of

APs they could sell to businesses, so they developed proprietary load balancing solutions. Additional discussions of these solutions are beyond the scope of this book and should be referred to your vendor of choice.

WarGames Wirelessly

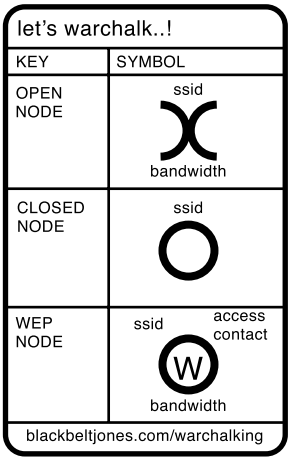
Like many of the beneficial technologies discussed in this book, wireless networks are also susceptible to a variety of threats; however, wireless is still a growing technology, and today you have the opportunity to protect and secure your network. This section takes a high-level look at some of those threats and why you should secure your network.

You might be familiar with the 1983 movie, *WarGames*, where a young man (played by Matthew Broderick) finds a back door into a military computer and unknowingly starts the countdown to World War III. The movie's young hacker executes this mayhem all over a modem, which coined the phrase ***WarDialing***.

Fast-forward almost twenty years when London-based author, Ben Hammersley was writing and he wanted a cup of coffee or even a bit to eat from the café across the street. Ben installed a WAP that gave him the wireless access he wanted; he was a giving man, however, and decided to let his neighbors know that they could have free wireless Internet access. Disappointingly, no one took him up on his generosity. Enter Ben's friend, Matt Jones, who posted a set of runes on a website (http://www.blackbeltjones.com) with the intention of creating a set of international symbols that would let people know that a wireless connection is available. Ben took a piece of chalk and drew these runes on the curb in front of the café and became the first WarChalker. (See Figure 8-3.)

Shortly after Matt posted these symbols on the Internet (a.k.a. Black Belt Jones), word spread fast and these two individuals started an Internet phenomenon resulting in new words with such ominous names as WarChalking, WarSpying, WarSpamming, and WarDriving—all ultimately a part of the evolution of wireless access. To clarify, none of these new terms enhance the security of your network. They are simply terms that attackers use to describe their activities. The following sections review each of these threats.

Figure 8-3 WarChalking Symbols



WarChalking

If you have ever seen a pirate movie in which a fancifully drawn treasure map displayed a large red X depicting where the ill-gotten gains were buried, you have some basic idea what role symbology has played in man's pursuit of riches. Much in the same way that the X marked the spot filled with gold, jewels, and silver, so did a series of runes depict areas of danger: which house a policeman might live in, or which houses were considered sympathetic to hobos during the great depression. For example, a rune in the shape of the pound sign "#" told fellow hobos that a crime had recently been committed and to avoid the area, or a casually drawn triangle might indicate that there were too many hobos working this area, so pickings were slim.

It was these "hobo hieroglyphics" from the Great Depression that inspired Ben and Matt to add a new dimension known as ***WarChalking***. WarChalking is a practice that originated with the intention of telling fellow wireless warriors where they could get a free wireless connection on a corporate or private wireless network. The symbols utilized by these "WarChalkers" generally indicate whether the wireless access point is considered "open" or "closed," depicted either by two half-circles back to back or a single regular circle, respectively, and what sort of security is protecting this access point.

WarChalking in its original form turned out to be a momentary cult-like movement that was fascinating for everyone. However, in practice it has changed significantly to reflect the realities of what people are trying to accomplish. Very few people walk around drawing marks on buildings; however, people are "chalking" maps using GPSs to show exactly where wireless access can be gained. Searching the Internet reveals quite a few online maps marked for use (http://www.netstumbler.com/nation.php). One of the added benefits of putting the maps online is that they are not washed away when it rains.

From a security perspective, it is highly unlikely that you will ever *see* the side of your building or sidewalk marked with a WarChalk symbol; however, it is likely that if your wireless network is not protected properly, it will appear chalked on someone's map for anyone to use. You might be wondering how attackers are finding these access points. Consider the last time that you saw anyone walking around with a laptop and a GPS. It does happen, but it might not be obvious because WarWalkers typically use backpacks to conceal their activities. In addition to the limitations posed by equipment battery life, all this walking can become tiring. Enter the next wireless threat—WarDriving—where converters can power a laptop for as long as the car is running.

note

WapChalking—A variant of WarChalking set up by the Wireless Access Point Sharing Community, an informal group with a code of conduct that forbids the use of wireless access points without permission. The group uses the WarChalking marks as an invitation to wireless users to join their community. In WapChalking terms, the two half-moon open node mark means that a wireless access device is currently indicating factory default settings and is thus easily detected.

WarDriving

WarDriving makes finding open wireless networks simple and dramatically increases the search area exponentially. The act of WarDriving is simple: you simply drive around looking for wireless networks. Part of the appeal is that you can

now use GPS systems connected to your laptop, which is then powered by your car. This makes the act of WarDriving accurate and potentially rewarding for those looking for your wireless network because they can cover a much larger area with a vehicle.

caution

Before delving too deeply into this subject, it is important to remember that WarDriving or "LAN jacking" an unwary subject's WAP is possibly illegal, depending on the part of the country in which you live. The reason you would consider even building an antenna in the first place is to remain as far away from the WLANs that you are sniffing in the first place. To get the latest information on legalities and updates on this front, consult your local computer club or perform an Internet search on "war driving and legalities."

It is disturbing that almost anyone can find your wireless network so easily, isn't it? Vendors turn everything on by default, regardless of network security concerns; this makes it easy for WarDrivers. By default, wireless access points broadcast a *beacon frame* that identifies (broadcasts the SSID) the wireless network they are a part of, every 10 milliseconds.

The average antennae on a wireless PCI card NIC is not sensitive enough to do a good job of zeroing in on low to medium-powered WAP signals, so many WarDrivers have resorted to using a USB wireless NIC outfitted with a homemade "directional Yagi" design antennae hardwired into the USB NIC, as shown in Figure 8-4 (http://3nw.com/pda/wireless/wi_fi_pringles_can_yagi_antenna.htm). Various designs yield better or worse results depending on the signal type of the wireless traffic you are trying to snoop. The wireless network is identified by a 32-bit character known as a ***Service Set Identifier (SSID)***. For a WarDriver, the easiest networks to find are those that are broadcasting this SSID. Perhaps I do not have any special applications but only a laptop with Windows XP. From a security perspective, Windows XP is wireless-aware and perhaps too friendly because it easily picks up any SSID broadcasts and automatically tries to join any available wireless network. With such a friendly operating system, who needs all the special tools?

Figure 8-4 Pringles Can as a Yagi Antenna

By default, the SSID is included in the header of the wireless packets broadcast every 10 milliseconds from a WAP. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device is not permitted to join the wireless network unless it can provide the unique SSID. Because an SSID can be sniffed from a packet in plain text, it does not supply any security to the network, even though it does function as a wireless network password. It is strongly recommended that WAPs have the broadcasting of their SSID disabled.

The presence of an SSID in a wireless network means that those engaging in the search should have more powerful wireless antennas that allow them to pick up and detect wireless signals. For example, if you want to "LAN jack" 802.11b/2.4-Ghz wireless network connections, you would most likely opt for a "helix" or "helical" design, which is basically tubular in design with a series of copper wire wrappings around a central core. This custom-made antennae style can be difficult to build because of its exacting standards and rather pricey parts list. On the other hand, a "wave guide" style can be made from rather inexpensive components such as a Pringles can (as shown in Figure 8-4), coffee can, or juice can.

The basic premise of building these specialty "signal stealers" is to mount them on the roof or hood of your car, connect the antennae to your wireless NIC, and drive around town looking for unsecured access points. Again, WarDriving for the purposes of stealing Internet access and snooping around a private network is

illegal and earns you a visit from men in blue suits with no sense of humor. WarDriving was invented by a man named Peter Shipley, who had the vision to take WarChalking to the next level:

> Most recently I invented Wardriving, while I am not the first person to go out and search for open wireless LANS (a few before me ventured around with in a with a laptop, pencil & paper manually scribbling notes). I was first to automate it all with dedicated software and a GPS. When I started this project the usage of WEP was around 15%, after going public with my findings, a year later WEP usage is now 33%. Thus it is good to know people are getting the message. Some maps I generated from these exercises can be found at *http://www.dis.org/wl/maps/*.

Depending on your frame of reference (and why you are reading this book), you might be wondering whether WarDriving is a crime. Of course, those doing the WarDriving do not view it as such; however, those of you who own the wireless networks might have a slightly different perception. While doing research, I stumbled across a quote—supposedly from the FBI—that states their position as follows:

> Identifying the presence of a wireless network may not be a criminal violation, however, there may be criminal violations if the network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal violations.

Therefore, if you are deploying a wireless network, you are likely to have someone try and find it, so your security depends on that individual's understanding that it is his responsibility to ensure that he does not violate any local, state, or federal laws that might pertain to his area. To slightly rephrase: you have gone through all the trouble of purchasing equipment, learning the process, loading the tools, and setting everything up. *Your* wireless network is not secured, and law enforcement expects the WarDriver not to do anything illegal. Are you prepared to leave your network vulnerable to those who do not support this law-abiding scenario? If you are, go back to Chapter 1, "Here There Be Hackers!" and start reading again!

The FBI quote seems to be an accurate representation of law enforcement agency positions on WarDriving; contests are held to see who can find the most wireless networks. Individuals involved in the wireless industry and dedicated to a certain bias in this debate, clearly maintain these websites, but check them out:

http://www.worldwidewardrive.org/

http://www.wardriving.com/

You will find links to various WarChalked maps that show the GPS locations and, in many cases, much more about open wireless networks worldwide. In doing my research for this chapter, I stumbled across a few people who have taken WarDriving to the next level, literally, in the form of WarFlying.

WarFlying

I have heard only of two cases of ***WarFlying***, but it is such an interesting endeavor that I just had to include it. WarFlying (a.k.a. WarStorming) is simply searching for wireless networks while flying in an airplane. However, because not many people have access to a small plane and the tools necessary to pull off WarFlying, the occurrences of WarFlying will be less than WarDriving. Because of the limited range of wireless LANs, the plane must fly below 1500 meters. WarFlying was first recorded in Perth, Australia.

WarFlying has some clear limitations because you do not have the ability (at least today) to triangulate on the access point, which could be several miles from where it was detected. Regardless, however, it is interesting, and I suggest checking out the three-part article on how Silicon Valley was WarFlown. I am not sure if that statement is grammatically correct; however, you get the point. Check out the rest of the story at http://www.arstechnica.com/wankerdesk/3q02/warflying-1.html.

WarSpamming

Everyone has received spam or junk mail; it is a plague on the Internet and, frankly, in my mailbox at home. I believe in free speech; however, that freedom does not give you the right to be heard. Fortunately, law makers and politicians

around the world are beginning to notice our feelings on this matter and developing laws to penalize spammers. These laws might or might not be effective—time will tell. However, is it is becoming more difficult for spammers to source their spam from countries that are beginning to develop these laws. There are also organizations that list IP addresses of places where spam has originated from, so what is a spammer to do? Many are now sourcing their spam from other countries; this presents all sorts of logistical problems and additional costs to our spammers. As a spammer, what if I could drive downtown or hire someone to find an open wireless network, join that network, and send my spam?

Remember the concept of downstream liability discussed in Chapter 3, "Overview of Security Technologies?" It would be simple to find an open wireless network and join it to send spam. The attacker (spammer) could be sitting in a café across the street, and you might never know. Now fast-forward a bit; the spam is sent to thousands of people who report that they received it, and yet another wrinkle–the spam was pornographic in nature. Yes, it can be even worse than that (remember, we are not talking about people who have morals—they are driven by other goals and needs). A quick check reveals your network's IP address, which is then blacklisted and reported to your ISP— and do not forget about the new antispamming laws. The result is that all outgoing e-mail from your company is blacklisted. How embarrassing when *your* customers get the bounce message saying that your company is spamming, the ISP shuts off your Internet connection, and law enforcement comes knocking. Also, if you have one of those Internet connections where you are billed by usage, expect a *big* bill this month.

The truth of the matter in ***WarSpamming*** is that your network did, in fact, spam others and, while it might have been as a result of an attacker, you are now liable because your wireless network was not secured properly. Who do you think is responsible for that and are they looking for a new job? Expect to see WarSpamming increase as it becomes more difficult for spammers to operate. Those who want to do questionable things will always find a way; some will stop as it becomes too difficult, and others will not.

WarSpying

A nice follow-up to WarSpamming is WarSpying, which is a relatively new phenomenon coming to a wireless video network near you. The most popular method of WarSpying is using those wireless X10 cameras. X10 is the camera featured in pop-up ads all over the Internet and they invariably have some gorgeous woman in them. X10 is also a means by which to automate your home, as in a smart house; however, that topic is beyond the scope of this book.

WarSpying was first documented in the magazine 2600, an interesting read if you can find the few nuggets of technical worth from the rants *it prints*. Regardless, it outlined how to make a wireless device that can pick up wireless surveillance systems transmissions. Since then, many people have explored and documented the topic online, and there are now reports of people tapping into all sorts of cameras that are transmitting over a wireless network. You can learn more about WarSpying at http://rhizome.org/RSG/RSG-X10-1/.

Notice I have completely avoided all discussions of the other nefarious uses into which this could develop. The key is *awareness* and an understanding of how to protect your network.

Many places that sell kits to start someone WarDriving—plans, maps, and so on are also readily available. A simple Internet search shows the results:

http://www.kenneke.com/index.html

http://www.hotspotlist.com/

http://www.wi-fiplanet.com/

This section was rather revealing about how wireless networks are found and, to a lesser degree, what some of the threats are. In addition, a variety of more specific threats are possible. Plus, after an attacker joins a wireless network, you have a host of other problems. The following sections examine these topics in more detail.

Wireless Threats

Wireless threats come in all shapes and sizes, from someone attaching to your WAP (Wireless access point) without authorization, to grabbing packets out of the air and decoding them via a packet sniffer. Many wireless users have no idea what kinds of danger they face merely by attaching a WAP to their wired network. This section discusses the most common threats faced by adding a wireless component to your network.

The airborne nature of WLAN transmission opens your network to intruders and attacks that can come from any direction. WLAN traffic travels over radio waves that the walls of a building cannot completely constrain. Although employees might enjoy working on their laptops from a grassy spot outside the building, intruders and would-be hackers can potentially access the network from the parking lot or across the street using the Pringles can antenna, as shown in Figure 8-2.

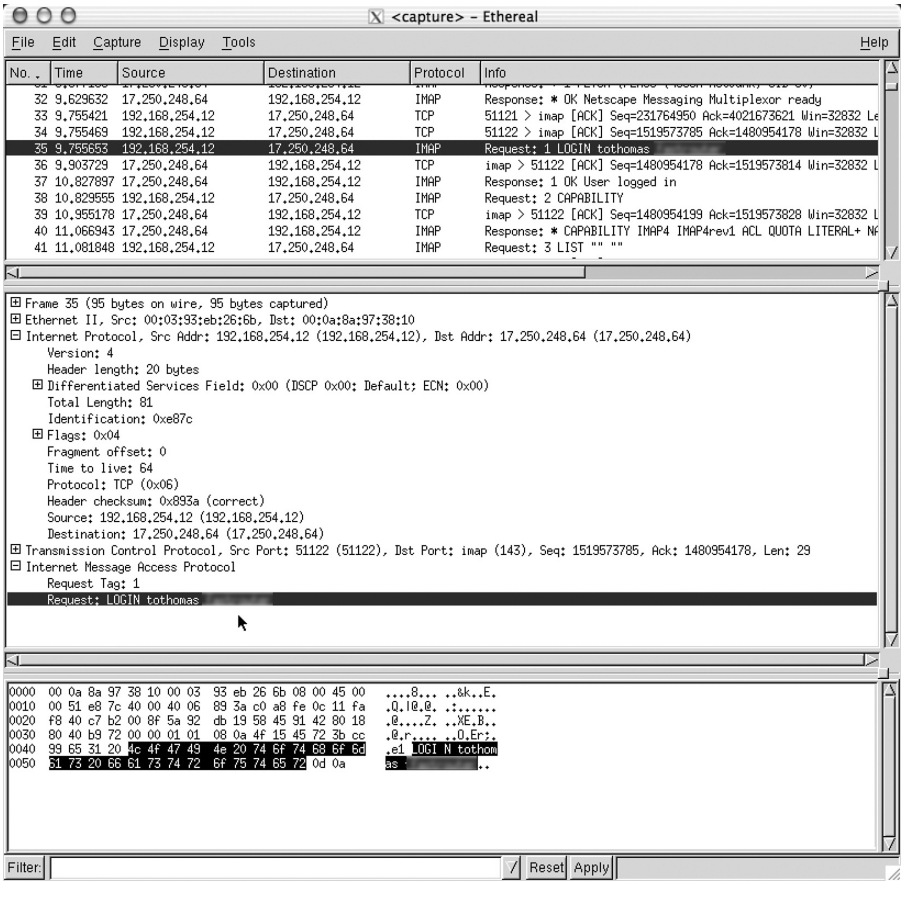
Sniffing to Eavesdrop

Because wireless communication is broadcast over radio waves, eavesdroppers who merely listen to the wireless transmissions can easily pick up unencrypted messages. Unlike wire-based LANs, the wireless LAN user is not restricted to the physical area of a company or to a single access point—the exception being those annoying areas that are not covered by the access, and it's always the office with a user who wants attention. The range of a wireless LAN can extend far outside the physical boundaries of the office or building, thereby permitting unauthorized users access from a public location like a parking lot or adjacent office suite. An attacker targeting an unprotected WAP needs only to be in the vicinity of the target and no longer requires specialized skills to break into a network. Anytime I do a network assessment for a customer in a shared office building, I almost always find one of two things:

- A neighboring business that has an open wireless network
- A neighboring user that has joined my customer's wireless network

If you want to examine the traffic going out over an Ethernet connection (wired or wireless), the best tool that comes to mind is the ubiquitous ***packet sniffer*** application. Packet sniffers allow the capture of all the packets going out over a single or multiple Ethernet connections for later inspection. These sniffer applications grab the packet, analyze it, and reveal the data payload contained within. The theft of an authorized user's identity poses one the greatest threats, and Figure 8-5 shows a freeware packet sniffer known as *Ethereal*, which is used on an Apple PowerBook G4 Laptop over a wireless Ethernet network to capture a mail application transmitting a username and password. (Names and passwords have been changed to protect the innocent, of course.)

Figure 8-5 Wireless Sniffer Packet Capture



The intent here is to show you how packet sniffers can be used against known behavior. In this case, when users start their computers, one of the first things they do is check e-mail. Most e-mail servers do not require any sort of encryption and, because the wireless network is not transmitting anything encrypted, the data is sent in clear text. An attacker with a packet sniffer could now *steal the user identity* and log in to the mail server as the unaware user anytime.

If you have read through packet captures before and are familiar with the information they contain, you should have immediately recoiled in horror at the knowledge that wireless networks are sniffers readily available and several are free. If this is the first time you have seen a packet capture, you might be in for a shock as you find out the wealth of information contained in a packet's data payload. Imagine if you were a domain administrator logging in to the domain and checking your online bank account or other information that could be critically damaging if someone hijacked it.

Denial of Service Attacks

Potential attackers who cannot gain access to your Wireless LAN can nonetheless pose security threats by jamming or flooding your wireless network with static noise that causes wireless signals to collide and produce CRC errors. These denial of service (DoS) attacks effectively shut down or severely slow down the wireless network in a similar way that DoS attacks affect wired networks. This vulnerability is apparent, and being on a wired network does not reduce your vulnerability to viruses, attacks, or in any other way increase security; in fact, it will quite likely get worse.

note

Restaurants, hotels, business centers, apartment complexes, and individuals often provide wireless access with little or no protection. In these situations, it is possible to access other computers connected to a wireless LAN, thereby creating the potential for unauthorized information disclosure, resource hijacking, and the introduction of backdoors to those systems. When users take corporate laptops home and use them on wireless networks, the vulnerabilities to your network increase. I have been on network assessments reviewing wireless usage and found that many a CEO, CFO, or CTO has the IT staff set up a wireless device at home for them with the same characteristics they have at work (SSID, and so on). This makes it easy for them to work at home with no trouble; however, the corporate network is extremely vulnerable because an attacker can go after a corporate employee's home network and compromise his machine. When the employee goes to work, so does the attacker— now he is inside your corporate network. Common sense is needed her—and a commitment by everyone in the management team to secure the network. This means not mixing corporate and home security.

Perhaps a bit more common is when other wireless devices unintentionally cause a denial of service to your wireless data network—for example, that new cordless phone running on 2.4 Ghz, or placement of access points near devices that generate interference and affect their operation, such as microwaves. Not all reduction in wireless connectivity is related to attackers, so remember that wireless networks are based on radio signals, and many things (walls, weather, and wickedness) can affect them.

Rogue/Unauthorized Access Points

WAPs can be easily deployed by anyone with access to a network connection, anywhere within a corporation or business. In fact, most wireless deployments are in the home so people with laptops can use them in any room in the house. The ease with which wireless technologies can be deployed should be a concern to all network administrators.

Because a simple WLAN can easily be installed by attaching a WAP (often for less than $100) to a wired network and a $50 WLAN card to a laptop, employees are deploying unauthorized WLANs while IT departments are slow to adopt the new technology. Unauthorized WAPS are known more commonly as ***Rogue APs***.

An executive of a large technology conglomerate was recently quoted as saying something like, "the hardest network to secure against wireless threats was one that had no wireless access at all" (or something very similar). What this executive meant was that, just because a company did not buy and install any wireless gear on their network did not mean that there wasn't any.

The concept behind wireless technology is to give people the freedom to roam around and still be connected to their network resources. The lure of this freedom is just too tempting to some folks in corporate America, so they go out and buy wireless gear on their own and hook it up to the office network. Now, you begin to see the problem.

note

In August 2001, Gartner Group reported that "at least 20 percent of enterprises already have rogue WLANs attached to their corporate networks" from authorized network users. Thus, risk-adverse organizations that consciously decide to delay WLAN deployment because of the security risks need to monitor their airspace to ensure that rogue WLANs do not inadvertently open a door for intruders. Stepping into the roll of the extremely paranoid, an attacker could be part of the cleaning crew in the evening and place a rogue access point into your network very easily.

If you can imagine how difficult it is to prevent people from bringing software from home and installing it on their work machines, it is ten times more difficult to prevent power users from "self adopting" wireless gear into the office LAN.

You might ask, "What is the harm in doing this?" The harm is that by installing an unauthorized access point, you have now extended an invitation to every hacker within a 500-foot radius to prowl your company's network, files, Internet access, printers, and any other devices currently connected to the private network.

Your network administrators take great pains to protect the corporate network from attackers and other "evildoers," and now there is a completely unprotected conduit into the company's holiest of holies: your internal corporate network.

A well-documented company has several security policies in place that govern every type of behavior when a user connects to the network. Rogue access points subvert these policies and open the doors to all varieties of bad things happening to the network.

To be perfectly fair to the employees who might commit this ultimate sin, it is important that the following information be made abundantly clear:

- Only authorized IT staff is to connect networking equipment.
- All devices that connect to the network, especially wireless access points, must conform to established security policies.
- Any devices that have been installed by anyone other than approved IT staff will become either the property of the company or will be rendered inert (that is, smashed into a million pieces).
- Hackers install rogue access points on a company network with the intention of stealing secrets and damaging data; this means no holiday bonuses because this kind of damage can cause a company to go out of business.

Finding rogue access points has become a little easier than in the past through the use of freely available software; the section entitled, "NetStumbler" delves into this. This same piece of software that made life easier for hackers has now become the favored tool of network security specialists for dealing with unauthorized wireless access points.

Attackers' Rogue AP Deployment Guidelines

I was going to call these "the rules for attackers to deploy rogue access points," but applying rules to those with criminal intent seemed an oxymoron. Attackers have developed some best practices that they have shared in their community and, by now, all honest network engineers are going to make WarDriving a frequent

occurrence to protect your network. Following is a brief list of what you can do to prevent attackers from "casing the joint":

- Know what you are trying to gain before placing the access point.
- Plan for the use of the access point; this means place so that if you have your laptop out and "working," you do not look suspicious.
- Place the access point as discretely as possible while maximizing your ability to connect to it.
- Disable SSID Broadcasting, thus requiring the target's IT staff to have a wireless sniffer to detect it.
- Disable all network management features of the access point, such as SNMP, HTTP, Telnet.
- If possible, protect the access point's MAC address from appearing in ARP tables.

The obvious disclaimer here is that these actions are not something you should ever do without—and I *really* stress this—*written permission***.** Many companies view even the accidental connection to their wireless network as an attack, so it is likely that you are going to be viewed as guilty until you prove your innocence.

It is also important to note that devices designed to jam radio signals have been around since before wireless ever became a standard. Because wireless is a radio frequency, it can be easily jammed.

Incorrectly Configured Access Points

Incorrectly configured access points are an avoidable but significant hole in WLAN security. Many access points are initially configured to openly broadcast SSIDs to authorized users. Many honest network administrators have incorrectly used SSIDs as passwords to verify authorized users. However, because the SSID is being broadcasted, this a large configuration error that allows intruders to easily steal an SSID and have the AP assume they are allowed to connect.

SSIDs act as crude passwords and are often used to recognize authorized wireless devices; thus, SSIDs should follow your corporate password policy and be treated as passwords. If you do not have a password policy, refer to Chapter 2, "Security Policies and Responses," and ensure the SSID cannot identify your company or business.

Network Abuses

Authorized users can also threaten the integrity of the network with abuses that drain connection speeds, consume bandwidth, and hinder a WLAN's overall performance. A few users who clog the network by trading MP3 files can affect the productivity of everyone on the wireless network. This ultimately leads to users who are trying to be productive complaining that the network is slow or that they keep losing connection. Based on experience, these types of issues are extremely difficult to identify and narrow down, especially if businesses decided to save money by using APs designed for home use rather than those designed for corporate use. Home-use APs do not come with the tools needed to help you.

Careless and deceitful actions by both loyal and disgruntled employees also present security risks and performance issues to wireless networks with unauthorized access points, improper security measures, and network abuses. Again, this recognizes the fact that the majority of security breeches and incidents come from inside, trusted individuals.

Wireless Security

You might be wondering why someone would want to use a wireless connection with all the insecurities that seem to go along with it. All is not lost, thanks to something known as Wired Equivalent Protocol, or is it Wireless Encryption Protocol—or it might even be Wired Equivalent Privacy. There seems to be some debate over exactly what WEP stands for among "industry experts." Regardless of how you spell or say it, WEP is an encryption algorithm that can be invoked to encrypt the transmissions between the wireless user and his Wireless access point (WAP).

From its inception, the 802.11b standard was not meant to contain a comprehensive set of enterprise level security tools. Still, the standard includes some basic security measures that can be employed to help make a network more secure. With each security feature, the potential exists for making the network either more secure or more open to attack.

Working on the layered defense concept, the following sections look first at how a wireless device connects to an access point and how you can apply security at the first possible point.

Service Set Identifier (SSID)

By default, the access point broadcasts the SSID every few seconds in beacon frames. Although, this makes it easy for authorized users to find the correct network, it also makes it easy for unauthorized users to find the network name. This feature is what allows most wireless network detection software to find networks without having the SSID upfront.

SSID settings on your network should be considered the first level of security and should be treated as such. In its standards-adherent state, SSID might not offer any protection against who gains access to your network, but configuring your SSID to something not easily guessable can make it more difficult for intruders to know what exactly they are seeing.

If you have your SSID configured to be any of the defaults cited in Table 8-1, you should change the SSID immediately.

Table 8-1 Default Wireless SSIDs

Manufacturer	Default SSID
3Com	101, comcomcom
Addtron	WLAN
Cisco	Tsunami, WaveLAN Network
Compaq	Compaq

continues

Table 8-1 Default Wireless SSIDs (continued)

Manufacturer	Default SSID
Dlink	WLAN
Intel	101, 195, xlan, intel
Linksys	Linksys, wireless
Lucent/Cabletron	RoamAbout
NetGear	Wireless
SMC	WLAN
Symbol	101
Teletronics	any
Zcomax	any, mello, Test
Zyxel	Wireless
Others	Wireless

A complete listing of manufacturers' SSIDs and even other networking equipment default passwords can be found at http://www.cirt.net/. As you can see, the SSIDs are readily available on the Internet, so it is a good idea to turn off SSID broadcasting as your first step.

Device and Access Point Association

Before any other communications take place between a wireless client and a wireless access point, the two must first begin a dialogue. This process is known as ***associating***. When 802.11b was designed, the IEEE added a feature to allow wireless networks to require authentication immediately after a client device associates with the access point, but before the access point transmission occurs. The goal of this requirement was to add another layer of security. This authentication can be set to either ***shared key authentication*** or ***open key authentication***.

You need to use open key authentication because shared key is flawed; although that is counter-intuitive, this recommendation is based on the understanding that other encryption will be used.

Wired Equivalent Privacy (WEP)

There is a lot of misconception surrounding WEP, so let's clear that up right away. WEP is not, nor was it ever meant to be, a security algorithm. WEP was never designed to protect your data from script kiddies or from more intelligent attackers who want to discover your secrets. WEP is not designed to repel; it simply makes sure that you are not less secure because you are not keeping your data in a wire. The problem occurs when people see the word "encryption" and make assumptions. WEP *is* designed to make up for the inherent insecurity in wireless transmission, as compared to wired transmission. *WEP makes your data as secure as it would be on an unencrypted, wired Ethernet network.* That is all it is designed to do, period; now your misconceptions are gone and you can move on. WEP can be typically configured in three possible modes:

- No encryption mode
- 40-bit encryption
- 128-bit encryption

WEP is an optional, agreed-upon encryption standard that is configured before the wireless user's connection to the WAP. After it is configured on the both the WAP and the user's end, all communications sent through the air are encrypted, thereby providing a secure link that is reasonably difficult to break, although recently developed hacker tools are gaining ground on this front. A side benefit of using WEP is that users wanting to connect to a WAP using WEP must have it enabled previously on their machine and have the "passphrase" or "key" that is shared between the end user and access point.

Wired Equivalent Privacy (WEP) was intended to give wireless users the security equivalent of being on a wired network. With WEP turned on, when each packet is transmitted from one access point to a client device, each packet is first encrypted

by taking the packet's data and a secret 40-bit number and passing them both through a encryption algorithm called RC4. The resulting encrypted packet is then transmitted to the client device. When the client device receives the WEP encrypted packet, it uses the same 40-bit number to pass the encrypted data through RC4 algorithm backward, resulting in the client receiving the data. Of course this process occurs in reverse and a client device is transmitting data to an access point. The encryption key used in this example was 40-bit, but 128-bit is also supported and, given the misconceptions and flaws with WEP, it is recommended that you always use the 128-bit encryption because it is better than 40-bit.

WEP Limitations and Weaknesses

WEP protects the wireless traffic by combining the "secret" WEP key with a 24-bit number (Initialization Vector, or IV), randomly generated, to provide encryption services. The 24-bit IV is combined with either the 40-bit or 104-bit WEP pass phrase to give you a possible full 128 bits of encryption strength and protection—or does it? There are a few issues surrounding the flawed current implementation of WEP:

- WEP's first weakness is the straightforward numerical limitation of the 24-bit Initialization Vector (IV), which results in 16,777,216 (2^{24}) possible values. This might seem large, but you know from discussions in Chapter 4, "Security Protocols," that this number is deceiving. The problem with this small number is that eventually the values and thus the keys start repeating themselves; this is how attackers can crack the WEP key.
- The second weakness is that of the possible 16 million values, not all of them are good. For example, the number 1 would not be very good. If an attacker can use a tool to find the weak IV values, the WEP can be cracked.
- WEP's third weakness is the difference between the 64-bit and 128-bit encryption. Perception would indicate that the 128-bit should be twice as secure, right? Wrong. Both levels still use the same 24-bit IV, which has inherent weaknesses. Therefore, if you think going to 128-bit is more secure, in reality, you will gain absolutely no increase in the security of your network.

Of course, freely available tools can accomplish all these things and are ready for the attackers to download and use as discussed in the section, "Essentials First: Wireless Hacking Tools," later in the chapter. Using WEP is better than nothing; however, layering the security of any part of your network is the key to safety and security, as has been established in all earlier chapters. Extensible Authentication Protocol (EAP) is the next level of security and is discussed in the correspondingly titled section.

MAC Address Filtering

MAC address filtering is another way people have tried to secure their networks over and above the 802.11b standards. A network card's MAC address is a 12-digit hexadecimal number that is unique to each and every network card in the world. Because each wireless Ethernet card has its own individual MAC address, if you limit access to the AP to only those MAC addresses of authorized devices, you can easily shut out everyone who should not be on your network.

However, MAC Address filtering is not completely secure and, if you solely rely upon it, you will have a false sense of security. Consider the following:

- Someone will have to keep a database of the MAC address of every wireless device in your network. If there are only 10–20 devices, it is not a problem. However, if you must keep track of hundreds of MAC addresses, this will become a nightmare quickly.
- MAC addresses can be changed, so a determined attacker can use a wireless sniffer to figure out a MAC address that is allowed through and set his PC to match it to consider it valid. Note that encryption takes place at about Layer 2, so MAC addresses will still be visible to a packet sniffer.

Extensible Authentication Protocol (EAP)

802.1X is a standard regarding port level security that the IEEE ratified. This ratification was initially intended to standardize security on wired network ports, but

it was also found to be applicable to wireless networking. ***Extensible Authentication Protocol (EAP)*** is a Layer 2 (MAC address layer) security protocol that exists at the authentication stage of the security process and, coupled with the security measures discussed thus far, provides a third and final layer of security for your wireless network. Using 802.1X, when a device requests access to the AP, the following steps occur with EAP:

1. The access point requests authentication information from the client.
2. The user then supplies the requested authentication information.
3. AP then forwards the client supplied authentication information to a standard RADIUS server for authentication and authorization.
4. Upon authorization from the RADIUS server, the client is allowed to connect and transmit data.

The four commonly used EAP methods in use today are

- EAP-MD5
- EAP-Cisco Wireless (also known as LEAP)
- EAP-TLS
- EAP-TTLS

The following sections provide a quick overview of each EAP method.

EAP-MD5

EAP-MD5 relies on an MD5 hash of a username and password to pass authentication information to the RADIUS server. EAP-MD5 offers no key management or dynamic WEP key generation, thus requiring the use of static WEP keys. This version of EAP does have some limitations:

- Because there is no dynamic WEP key generation available, the added use of EAP provides no increased security over WEP. Attackers can still sniff your airborne traffic and decrypt the WEP key.

- EAP-MD5 does not provide for a means for the client device to ensure that it is transmitting to the proper access point. A client could erroneously transmit to a rogue access point.

Because EAP-MD5 offers no other features over the standard 802.1X, EAP-MD5 is considered the least secure of all the common EAP standards.

LEAP (EAP-Cisco)

EAP-Cisco Wireless, or LEAP as it is more commonly known, is a standard developed by Cisco in conjunction with the 802.1X standard and is the basis for much of the ratified version of EAP. Like EAP-MD5, LEAP accepts a username and password from the wireless device and transmits them to the RADIUS server for authentication. Cisco added additional support beyond what the standard required, resulting in several security benefits as follows:

- LEAP authenticates the client; one-time WEP keys are dynamically generated for each client connection. This means that every client on your wireless network is using a different dynamically generated WEP key that no one knows—not even the user.
- LEAP supports a RADIUS feature called session timeouts, which requires clients to log in again every few minutes. Fortunately, this is all handled without the user having to do anything. Couple this feature with dynamic WEP keys, and your WEP keys will change so often that attackers will not be able to determine the key in time.
- LEAP conducts mutual authentication from *client-to-access point* and *access point-to-client*; this stops attackers from introducing rogue access points into your network.

There is presently a single known limitation to running LEAP.

MS-CHAPv1 is used for both the client and access point authentication and is known to have vulnerabilities.

note

Not everyone has a RADIUS server that is ready to utilize LEAP; however, Cisco access points can be configured with a feature called local AAA Authentication on a per user basis. This allows the user database to reside in the AP instead of RADIUS and works well if you have only a limited number of users.

EAP-TLS

Microsoft developed EAP-TLS, which is outlined in RFC 2716. Instead of username/password combinations, EAP-TLS uses X.509 certificates to handle authentication. EAP-TLS relies on transport layer security to pass PKI information to EAP. Like LEAP, EAP-TLS offers the following:

- Dynamic one-time WEP key generation
- Mutual authentication

The drawbacks of EAP-TLS include the following:

- PKI is required to use EAP-TLS; however, most companies do not deploy PKI.
- Microsoft Active Directory with a certificate server can be used; however, change is difficult in this model.
- If you are using Open LDAP or Novell Directory Services, you need a RADIUS server; again, not everyone has immediate access to one.
- If you have implemented PKI using VeriSign certificates, all the fields required by EAP-TLS are not present.

Unless you are ready to follow the implementation of EAP-TLS exactly as Microsoft has laid it out, you should probably look for another method.

EAP-TTLS

Funk Software (http://www.funk.com/) pioneered EAP-TTLS as an alternative to EAP-TLS. The wireless access point still identifies itself to the client with a server certificate, but the users now send their credentials in username/password form. EAP-TTLS then passes the credentials in any number of administrator specified challenge-response mechanisms (PAP, CHAP, MS-CHAPv1, MS-CHAPv2, PAP/Token Card, or EAP). The only challenges to EAP-TTLS are

- The slightly less secure than dual certificates of EAP-TLS
- The upcoming standard developed by Microsoft and Cisco that works exactly the same way—Protected EAP (PEAP)

Increasing Wireless Security

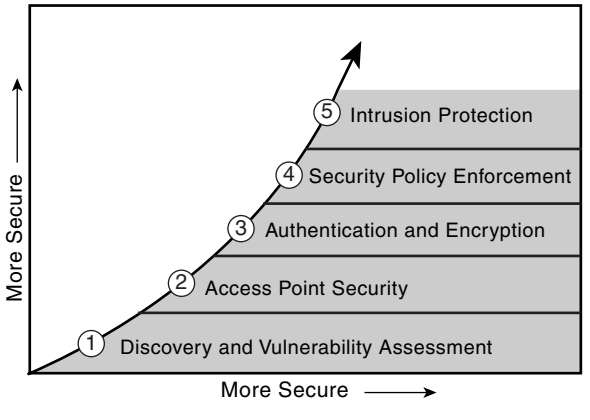
As discussed, there are some possible means of securing your wireless network beyond WEP. It is unlikely, however, that anyone has a RADIUS server ready and waiting to be used; therefore, you need to identify steps you can take immediately to increase the security of your wireless network. The attention on the pitfalls of wireless LANs has inspired some organizations to ban wireless LANs altogether. However, security-conscious organizations are fortifying their wireless LANs with a layered approach to security that includes the following:

- Putting the wireless network behind its own routed interface so you can shut off access to at a single choke point if necessary
- Discovery of rogue access points and potential associated vulnerabilities
- Physical and logical access point security to ensure that someone cannot walk up to an access point and alter its configuration without your knowledge
- Changing the SSID and then picking a random SSID that gives away nothing about your company or network
- Disabling active SSID broadcasting
- Rotating your broadcast keys every ten minutes or less

- Encryption and authentication, which might include a virtual private network over wireless
- Using 802.1X for key management and authentication
- Looking over the available EAP protocols and deciding which is right for your environment
- Setting the session to time out every ten minutes or less
- Establishing and enforcing wireless network security policies
- Implementing proactive security measures that include intrusion protection

As shown in Figure 8-6, these steps and recommendations can be illustrated as a phased approach, which enforces the concept of first knowing what the vulnerabilities are and moving forward from that point.

Figure 8-6 Stages of Securing Your Wireless Network



Essentials First: Wireless Hacking Tools

This section examines some of the tools that eliminate some of the threats discussed in the preceding sections. In theory, these tools were all designed to help network administrators take care of their networks, and they are still touted as

such on each website. In reality, these are some of the same tools that attackers can and will use; thus, network administrators should also use them to ensure that their wireless networks are secure.

NetStumbler

Wireless networking is everywhere! That is not meant as hyperbole—it really is *everywhere*. Wireless technology uses radio waves to transmit data, so wireless packets are probably flowing in the air in front of you as you read this.

As everyone knows by now, where wireless packets flow, wireless access points are pumping them out (where there is smoke, there is fire). If only there was a way to find out whether any WAPs were nearby. Fortunately (and unfortunately), there is a way to discover just that.

A little piece of freeware called Net Stumbler is available on the Internet (found at: http://www.netstumbler.com/) that provides you with such secret pieces of information as the following:

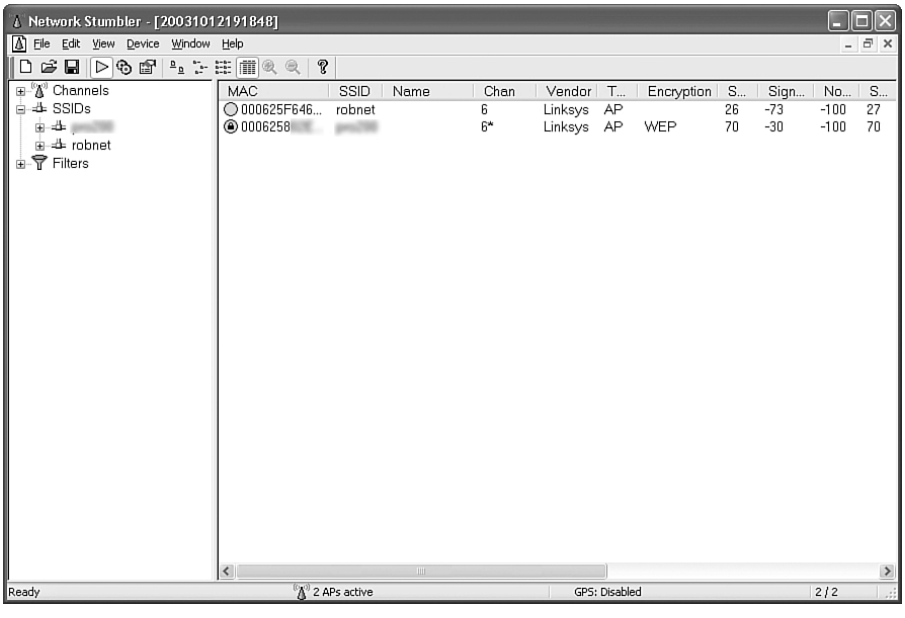
- WAP's SSID (Service Set Identification, the unique name you can assign to your WAP)
- Signal strength of the discovered WAPs and whether the WAP is using WEP

What channel the WAP is transmitting on, and some other sneaky bits of information

note
NetStumbler is also available for Apple computers in the form of an application known as MacStumbler (http://www.macstumbler.com).

You might have even seen NetStumbler make an appearance on the local evening news under the headline, "Wireless Security Threats: You Could Be Next!" or some other scary tagline. Figure 8-7 shows the NetStumbler interface.

Figure 8-7 NetStumbler Scanning



NetStumbler sends out a broadcast on all channels looking for a response. If your WAP is configured to respond to the broadcast (SSID broadcast "enabled" setting), NetStumbler logs that WAP and furnishes you with a "bing-bing" tone designating a target. A word of caution, however: NetStumbler can lock only onto 802.11b and some 802.11a-compliant WAPs.

The truth is that NetStumbler does not tell you much more than your wireless NIC's configuration interface. However, the trick is that NetStumbler tells you all the information you need about someone else's wireless network.

Most wireless NIC configuration programs allow you to perform a ***site survey***, which sniffs around for other wireless access points that are configured to broadcast on the same channel as your NIC. If you happen to find a WAP with the default SSID (in this case, the default SSID of a Linksys WAP is "linksys") displayed, you can assume that you can connect to that WAP with little or no trouble.

One of the best features about NetStumbler is its capability to integrate laptop-based GPS units into its WAP discovery adventure. Imagine driving along with your trusty laptop on the passenger seat of your POV (privately owned vehicle) and hearing the pleasant "bing-bing" tones generated by NetStumbler as it happily sniffs out WAPs within transmitting distance. Every time that your laptop makes that sound, NetStumbler queries the attached GPS unit and records the coordinates of the WAP it found. Later, you can download the coordinates into mapping software and have a nice, little map printed out to show you where the WAPs were found. And who says technology doesn't make our lives just a wee bit more interesting?

The whole GPS issue aside, NetStumbler is not actually a hacking tool because the information it reveals is just a step above what your NIC can already help you find out. Tools like NetStumbler are more along the lines of a "reconnaissance" tool because they help you discover things that might not have been immediately obvious. One mission that NetStumbler has recently been assigned is that of Rogue AP detector.

Wireless Packet Sniffers

Sniffing packets can be both fun and profitable if you know how and what to sniff. Any network administrator can lay his hands on a packet sniffer in a matter of seconds and snag a couple of hundred packets before you can even read this paragraph. The contents of these packets can reveal network secrets that have been closely guarded. "Sniffing," or "snarffing" in the HaXoR world, is the process of intercepting and recording traffic that was never supposed to be seen by anyone other than the sender or receiver.

To the layman, the idea of "sniffing," "capturing," or "snagging" packets is an alien concept; therefore, the basics of the operation deserve some brief discussion:

1. Packets travel over an Ethernet connection from source to destination.
2. A NIC set to "promiscuous" mode can "listen in" on all local traffic.
3. A packet "sniffer" can see and record all this traffic.

4. A packet "sniffer" can also decode the packet and display neat things like the source MAC address, the destination MAC address, and the data payload contained in the packet.
5. Packets contain things like unencrypted Windows LanMan v.1 passwords, passwords sent in clear text, and other tasty things relished by hackers.

Now that you know about wired packet sniffers, you also need to meet their wireless cousins. How is this possible, you ask? Can I really capture wireless packet traffic? Could it be that easy? Do hackers know about this? The answers are, yes, yes, and *yes*.

Yes, hackers know about sniffing wireless connections, and they have made the most of it. Have you turned on a MAC filter on your WAP? Packet captures rat you out by telling the hacker the MAC address' source. It is easy to spoof a MAC address on your wireless NIC, especially with a program called SMAC, lovingly created by a group of guys at KLC Consulting. They make both a Win32 and Linux version of the software that virtually (as in not actually, but makes it appear so) changes your NIC's MAC address. If a hacker "sniffs" your wireless packets, he can decode the packets, read the MAC address of a machine listed in the WAP's MAC filter, plug that number in SMAC, and impersonate a machine that is authorized to use the WAP. It can do all this in less than one minute. That is correct—60 seconds. In the time it takes to dip a biscuit in gravy and eat it, a hacker can intrude on your network. But what if I am running WEP, you might ask? Read the following section and save your question for later (http://www.wildpackets.com/products/airopeek_nx).

AirSNORT

Now you understand more about the encryption used by WEP, how WEP does its thing, and how wireless is vulnerable. Things were going along swimmingly back in the year 2001 for the wireless world—until a piece of software called AirSNORT came along. The 802.11 protocol was under attack and that attack continues even today.

AirSNORT made its first widespread public appearance in the pages of *Wired* magazine on August 20, 2001. The concept of snagging packets and cracking the encryption protecting them was not a new concept; in fact, security experts had known of WEP's weaknesses for quite a while. The AirSNORT software was merely the hacker's "combo meal" that put the capture and the cracker in one easy to use application. The downside to AirSNORT was that it ran only on Linux (and still does today), which did not have nearly the level of acceptance that it does today.

The people who invented AirSNORT were interviewed at the time of release and professed that it was not written with the intention of it becoming a staple in the hacker toy box; rather, it was intended to be a proof of concept tool that demonstrated the inherent weakness of WEP.

It is estimated that AirSNORT needs to capture only five or six million packets and chew on them for as little as a minute, or as long as a couple of hours, before it can chew through the encryption and reveal the WEP key. Those time estimates were unbelievable in 2001. Can you imagine how much faster today's 2- and 3-gigahertz machines can mow through the same amount of data? Can you say s-e-c-o-n-d-s? From an attacker's point of view, the downside of this is that it can take a long time to gather the millions of packets necessary—but once they do….

As if this were not bad news enough for would-be wireless warriors, another piece of software called WEPcrack popped on the radar screen at the same. WEPcrack did roughly the same job as AirSNORT, but it was not as far along in the development phase. You can find AirSNORT at: http://airsnort.shmoo.com/.

note

Other wireless tools such as KisMET and KisMAC, which are wireless AP locators and include support for GPS location and positioning, can be used to create maps of all known, open wireless access points in a city.

Chapter Summary

This chapter has hopefully shed some light on the technology that drives wireless and the first steps for beginning to secure a wireless network. There are a variety of areas surrounding wireless that you should be concerned about; however, there are clear, layered steps that can be applied to secure a wireless network with minimal impact to users. Of utmost importance are the steps you take today to increase security that will not hamper or affect the security of your wireless network. The chapter concluded with a discussion of the *freely* available tools relating to attacking and securing wireless networks. Attackers commonly use these tools; more importantly, however, those who are looking to find flaws in their wireless network security *should* use them to patch them up and prevent easy attacks.

Chapter Review Questions

1. How are the terms 802.11 and Wi-Fi used? In what ways are they different or similar?
2. What are the five benefits to organizations that would provide reasons for them to implement a wireless network?
3. WarDriving is the most common means of searching for wireless networks. What is needed to conduct a WarDrive, and why is it so useful for attackers?
4. What is one type of freely available wireless packet sniffers?
5. Are wireless networks vulnerable to the same types of denial of service attacks as wired network? Are they vulnerable to any additional attacks that wired networks are not?
6. What are the four types of EAP available for use?