

# Chapter 9: Wireless Vulnerabilities and Attack Methods

## Overview

Describe the following types of WLAN security attacks, and explain how to identify and prevent them where possible:

- ◆ Eavesdropping, Man-in-the-Middle, and Hijacking Attacks
- ◆ Denial of Service (Physical and Data Link Attacks)
- ◆ Management Interface Exploits
- ◆ Encryption and Authentication Cracking

WLANs have vulnerabilities that are common to all computer networks, and they have vulnerabilities that are specific to IEEE 802.11 networks. When something is implemented in the same way over and over again, it becomes more likely that someone will eventually discover the weaknesses in that thing if weaknesses exist.

This is seen in the most popular operating systems and software applications, and in the most popular WLAN networks, which are IEEE 802.11 based.

IEEE 802.11 networks showed their biggest security vulnerability when the one real security feature was hacked in the first few years of its existence. This security feature was WEP (discussed later in this chapter and the [next](#)). Other optional configuration parameters have been touted as security features over the years, but either they were never intended as such or vulnerabilities were known from their inception.

These features include things like MAC filtering and disabling the broadcast of SSIDs from access points. As you will see, in these next two chapters, neither of these features provide any real security.

This chapter will present the inherent weaknesses in standards-based IEEE 802.11 networks that do not implement the newest version of Clause 8 in a secure fashion based on the solutions first introduced in the IEEE 802.11 amendment.

## Identifying and Preventing WLAN Security Attacks

Clause 8 was included in the original IEEE 802.11-1997 standard; however, it only offered the use of authentication mechanisms and WEP encryption that were shown to be very weak very quickly.

With the ratification of the IEEE 802.11i amendment, Clause 8 has been heavily updated to include support for better security technologies that can eradicate (at least for now) the majority of the security vulnerabilities discussed in this chapter. A robust security network as specified in the new version of Clause 8 that is implemented with a strong EAP type is very difficult, if not impossible to hack into at this time.

The original Clause 8 only spanned about 11 pages, whereas the new clause is almost 100 pages long. There is obviously more information included, and so far, it has proved to provide a security framework that is very strong.

In this section, we will study the common attack methods used against WLANs. These methods include:

- ◆ Eavesdropping
- ◆ Hijacking
- ◆ Man-in-the-middle
- ◆ Denial of service (DoS)
- ◆ Management interface exploits
- ◆ *Encryption cracking*
- ◆ *Authentication cracking*
- ◆ MAC spoofing
- ◆ Peer-to-peer attacks
- ◆ Social engineering

### **Eavesdropping**

Because a WLAN sends data through the open air, an antenna placed in the right location and connected to a WLAN NIC can read this data. It is impractical to prevent an attacker from "reading the frames" out of the air, if the attacker can get close enough to your WLAN to pick up the signal.

He will not have to associate with the WLAN to view the frames that are being transmitted, and this is very important to remember. If you just read that last paragraph and begin to think, "Wait. I thought you could encrypt the data," you are absolutely correct.

You can encrypt the data, but I can still read the frames using a WLAN analyzer application. I may not be able to decipher the meaningful data that is in the frames, but I can read the frames, and that cannot be stopped. Since you cannot stop an attacker from reading the frames, you must ensure that you are using an encryption method that is solid enough to protect against a fast attack.

In other words, if an attacker can hack your encryption in just a few minutes, it's not strong enough. As you may know, WEP encryption can indeed be hacked in just a few minutes and should not be used in any production WLAN when newer encryption schemes are available.

Some people refer to wardriving as casual eavesdropping. *Wardriving* is the process of locating WLANs that have not been configured for your access. In recent years, it has evolved to act as an umbrella term for nearly any method used to find a WLAN.

Some wardriving may be innocent in intent, but this does not make it any more legal. You should avoid accessing or penetrating WLANs that were not set up for your use or on which you were not granted permission to perform testing.

If you drive down the street in the neighborhood and find and use an open WLAN—either intentionally left open or unintentionally may actually be committing a crime, depending on local regulations. This is a very serious issue and will likely grow to become more serious as time passes. When you access a network, be sure you've been given the right to do so—even if you are performing a penetration test.

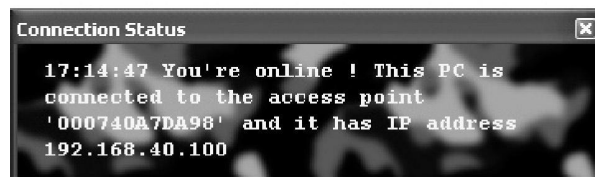
In the situation where you've been asked to perform a penetration test, I suggest you acquire a written contract that stipulates what and how you will be allowed to access the network. Others suggest that wardriving does not even fit into the category of eavesdropping, since you are not actually "listening" to meaningful conversations.

For our purpose here, we can categorize wardriving as eavesdropping because the wardriver is listening for frames that are not intended for his or her use. That is the fundamental definition of *eavesdropping*: the intercepting and reading of messages and information by unintended recipients.

The following tools may all be used for casual eavesdropping or WLAN network location:

- ◆ MacStumbler
- ◆ KisMac
- ◆ NetStumbler
- ◆ KisMet
- ◆ Easy WiFi Radar

There is a more sinister type of eavesdropping, however. This malicious type of eavesdropping involves the capture of data packets that are traversing the wireless medium (WM). In order to do this, the attacker will need to utilize a WLAN protocol analyzer. This is a software application that is designed for or also supports the capturing of IEEE 802.11 frames through a WLAN NIC.



Many regulatory domains have finalized laws making it a crime to listen in telephone conversations without previous authorization.

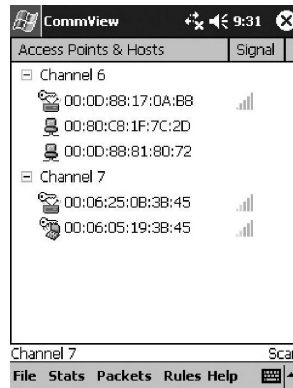
The recording of telephone conversations, even those initiated voluntarily by the customer, is illegal in the United States. This is why you hear the message, "This call may be recorded," when you call so many customer service support centers. A number of these regulatory domains have extended these laws, or written new ones, that cover all electromagnetic communications.

Since WLANs use electromagnetic waves for communications, their frames would be covered under such regulations. Don't take these laws lightly. Though there have not been many reported cases of prosecutions up to this point, this should not be taken as a sign that governments will not enforce these laws.

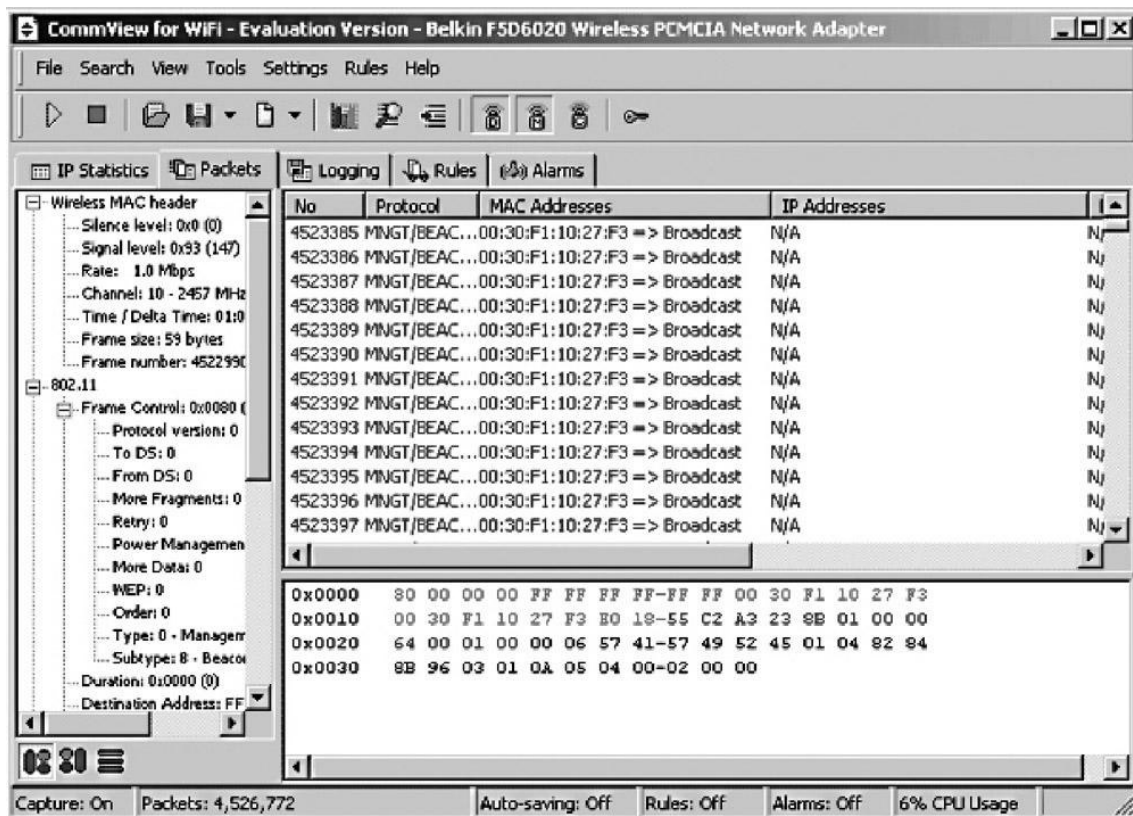
There are both commercial and freeware applications that can be used for malicious eavesdropping. Applications are available for the Windows, MAC, and Linux platforms. The following list includes some of the more common WLAN protocol analyzers available today:

- ◆ OmniPeek Personal (free)
- ◆ AiroPeek (commercial)

- ◆ Network Instruments Observer (commercial)
- ◆ AirMagnet Laptop Analyzer (commercial)
- ◆ Javvin CAPSA (commercial)
- ◆ Ethereal (open source), now Wireshark
- ◆ CommView for Wi-Fi PC (commercial)
- ◆ CommView for Wi-Fi PocketPC (commercial)
- ◆ Wireshark (free)



CommView for Wi-Fi application running on a PocketPC. This tool is mostly used for wardriving, since it is limited in the data it can retrieve.



## Hijacking

*Hijacking* is a situation in which an unauthorized user takes control of an authorized user's wireless LAN connection. In a WLAN, hijacking is done at Layer 2 for DoS and at Layer 3 for attacking purposes, although you could perform certain DoS attacks with a hijack of Layer 3 as well. The process of hijacking Layer 2 (the MAC layer) is outlined here:

1. The attacker starts his own AP, usually through software running on his computer.
2. The attacker configures his AP to use the same SSID as the WLAN to which the victim is currently associated.
3. The attacker sends a deauthentication frame (or turns on a high-powered RF signal generator, causing interference that results in the victim needing to reassociate), forcing the victim to look for a new AP with which to associate.
4. Since the attacker's AP is closer and provides a stronger signal, the victim associates with the attacker's AP and the user of the machine doesn't realize he is no longer associated with the valid AP.

If we stop at this stage, the result is a DoS scenario. Because the victim is no longer connected to the AP that actually provides access to needed services, services have been denied. However, the attacker can run a DHCP server on his machine that provides an IP address to the victim's STA.

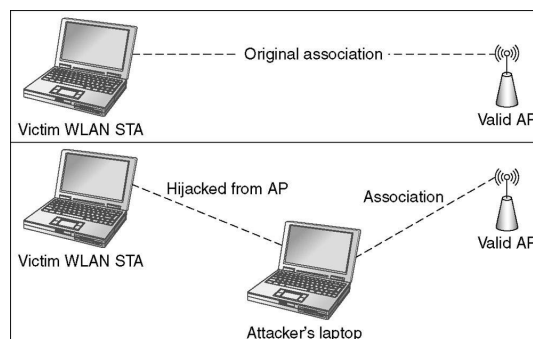
After the victim STA has a working IP configuration, the attacker can then attempt to access the victim station to steal data or plant viruses, worms, and more.

The attack can be taken to another level. At this level, the attacker uses two WLAN NICs. One acts as the AP to hijack Layer 2, as outlined in the four preceding steps, and the other acts as a standard WLAN client of the valid AP to which the victim was originally associated.

The attacker then allows bridging across the two WLAN NICs, which is supported by a number of operating systems like Windows XP. With this latter configuration, a *man-in-the-middle* attack is successfully accomplished.

The victim can continue to browse the Internet or use other services provided by the valid AP. At the same time, the attacker can launch various attacks against the victim STA or simply monitor the traffic that is passing through the newly arranged bridge path through his computer.

When you configure such a man-in-the-middle attack, you have hijacked Layers 1, 2, and 3 and have the ability to continue attacking the victim STA, without the user realizing that anyone is even accessing his computer.



## Windows Client Vulnerabilities

In addition to the hijacking concept presented here, Windows clients introduce an interesting vulnerability. By default, many Windows clients send out probe requests looking for "preferred networks."

These are networks that you've connected to in the past; they can be seen in the Wireless Networks tab of the Properties dialog for your wireless connection in the Network Connections container.

The order in which they appear is the order in which Windows attempts to connect to these networks. If the client cannot find a preferred network from this list, it will not simply stop scanning. Instead the client will scan for a randomly chosen network based on a randomly generated SSID.

While this behavior may seem odd, it was implemented with good intentions. If there were no preferred networks available, the client would need to power off the WLAN device and then power it back on in order to scan for preferred networks again at some interval.

Rather than having the user notified of a device being turned on and off, the developer chose to leave it on and probe for an assumed unavailable network with a random SSID. It didn't take long for security crackers and hackers to realize the vulnerability exposed.

While standard APs are configured with a specific SSID that they listen for in probe requests and transmit in Beacon frames (by default), new softwarebased APs can respond to any probe request and say, "Yeah, that's me. I'm the SSID you are probing for." In other words, cracking tools are out there that allow you to set up a rogue AP that responds to any SSID for which a client is probing.

Now, when a Windows client probes for the randomly generated SSID, the rogue AP can even respond to this. An example of such a cracking tool is the softwarebased AP named Karma on the Linux platform. The only real protection you have against such attacks (when using the Windows default client) is to keep your WLAN card powered off when you're not using it and be sure to remove any unsecured wireless networks from your preferred network list immediately after using them. If any unsecured wireless networks exist in your preferred network list, your computer will associate with an unsecured software based AP running Karma (or some other tool) automatically.

This remote attack machine can provide your computer with an IP address, and then the attacker can begin launching an attack against your machine. Another prevention technique would be to use a different WLAN client from the builtin Windows client. Many people are still unaware that you can disable the builtin Windows client and use a thirdparty WLAN client application that provides much greater security.

## Denial of Service

Denial of service attacks are launched specifically against WLAN networks at Layer 1 (Physical) and Layer 2 (Data Link). A *denial of service* attack is a category of attacks that includes any actions resulting in the inability of users or systems to access needed resources. DoS attacks can be simple to implement or very complex.

For this reason, they can be launched by attackers with little skill as well as attackers with in-depth knowledge of IEEE 802.11 networks. The Layer 1, or Physical layer, attacks are also known as *RF jamming* attacks.

This is done using devices that output RF energy, usually across the entire 2.4 GHz spectrum used by IEEE 802.11 devices. When these intentional radiators put out the RF

energy at the power levels they support, it drowns out the RF energy being transmitted by valid STAs on your WLAN. Since the device (called a signal generator) puts out a signal that drowns out the signals of the WLAN, it effectively causes a DoS scenario.

The interference can also be narrowband and still cause problems on your WLAN if the band fits nicely in the center of your configured IEEE 802.11 channel. Since the AP will not likely be configured to automatically adjust its channel in the face of interference (though some APs do have this capability), a DoS scenario can even be caused by narrowband signal generators.

Unintentional DoS scenarios can also exist due to the interference caused by microwave ovens, cordless phones, and other devices that share the frequency bandwidth with the WLAN. These unintentional DoS scenarios can wreak havoc on your WLAN even though they are not malicious.

In general, they can be detected through the reports that come in from your users of degraded performance on the network. If these complaints begin to surface suddenly, it could be an indicator that something has changed in your environment. Look for new microwaves, new cordless phones, or even new WLANs installed by employees or nearby organizations.

Because signal generators are somewhat expensive, Layer 1 DoS attacks are not usually as common as Layer 2 DoS attacks on WLANs. A Layer 2 attack is launched by exploiting the processes used for frame management and network communications in a WLAN. For example, an attacker may spoof a deauthentication frame. This means that the attacker generates a frame on the WM that uses (spoofs) the MAC address of the AP, and the frame generated is a deauthentication or disassociation frame.

These frames are management frames and, more specifically, notification frames. They cannot be ignored by the client STAs, so the client stations will be denied access to the WLAN as long as the attacker continues to transmit the spoofed disassociation or deauthentication frames.

There are additional Layer 2 DoS attacks that can be executed against a WLAN. You do not need to understand the details of their functionality for the CWNA exam, but it is helpful to know they exist. These additional methods include:

- ◆ PS Pool floods
- ◆ Association floods
- ◆ Authentication floods
- ◆ Empty data floods

The last one, empty data floods, is possible because you can use many different tools to generate data packets. If you install two or three WLAN adapters in a laptop computer and then enter any WLAN area, you can generate data frames of the maximum frame size on a continual basis.

Since you are doing this with three different adapters at the same time, chances are good that you will tie up most of the available throughput in the service area. The closer you are to the AP and the more powerful the output of your WLAN adapters, the more likely you are to consume a large portion of the network's throughput.

This is often said to be a data flood attack instead of a Layer 2 attack because the frames are intended to be used to carry upperlayer data and, in fact, they are generated by

applications residing at the upper layer of the OSI model. For this reason, this is usually called a data flood attack, but a data flood attack is at least a partial DoS attack as well.

Eventually, the IEEE 802.11 standard will include protected management frames, and this will help prevent the true Layer 2 DoS attack methods. The IEEE P802.11w draft is in version 1.0 at the time of this writing. Much like the IEEE 802.11i amendment, the IEEE 802.11w amendment defines more robust methods to be used in WLANs.

Where 802.11i specifies a robust security network, P802.11w defines robust management frames. In fact, P802.11w is written in such a way that it depends on 802.11i as an existing entity in the standard. For this reason, the draft document for P802.11w states that it is based on the draft for the rollup assumed to be released sometime in 2007 as IEEE 802.11-2007.

For now, the use of a spectrum analyzer will help you track down the location of the interfering device. You may find an individual in the parking lot with a signal generator, or you may find that one of your users has installed a rogue AP in the corner of his office and configured it to use the same channel as your WLAN. Since he is sitting so close to the AP, he hasn't really noticed much of an interference problem, particularly since he is the only one using it. This is actually more common than finding the attacker with the signal generator at least in my experience.

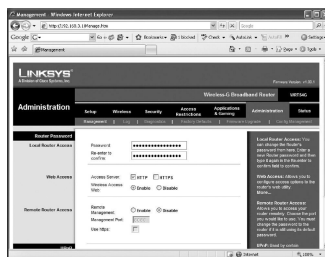
## Management Interface Exploits

Most APs support a web based management interface. When an attacker connects to an open WLAN, one of the first things she will usually do is attempt to connect to  $x.x.x.1$ , where the  $x$  represents the portion of the IP address in that octet. In other words, she will look at the IP address assigned to her machine.

Imagine it is 10.10.10.18. She will attempt to connect to 10.10.10.1 with her web browser. This is because a WLAN residential gateway and many wireless routers use this IP addressing scheme for their default configuration.

Some APs default to an IP address of 10.0.0.2, and others default to 192.168.1.245. However, most enterprise APs will have IP addresses assigned by the WLAN administrator. As an attacker, however, all she has to do is attempt to connect to each IP address in her subnet (determined by inspecting the IP address and subnet mask in her received configuration) or use a scanning tool that will attempt to connect to port 80 on each IP address.

In short order, she will likely find the webbased interface of the AP or WLAN router if it is enabled. One of the simplest solutions to this problem is to disable the webbased administration interface for WLAN connections. You must also consider the other configuration methods such as telnet and SSH. Be sure they are either disabled or secured with passwords that are very difficult to guess.



It is not uncommon for an attacker to turn a *management interface exploit* into a type of DoS attack. I've seen multiple scenarios where the attacker gained access to the AP or WLAN

router and then configured the MAC filters to only allow his or her client access. This gave the attacker full access to the provided throughput for some period of time until the exploit was discovered.

In all of these cases that I've encountered, the WLANs were wide open and had not implemented any effective security solutions. WPA-PSK or WPA2-PSK with a sufficiently long and cryptic preshared key would have prevented the attack in every one of these scenarios. Two of the organizations were large enough to justify implementing WPA2-Enterprise and use very strong levels of encryption and authentication.

## **Authentication Cracking**

With the weaknesses found in the WEP implementation, the IEEE began development of a more secure authentication and encryption algorithm. While they were developing what eventually became an amendment to IEEE 802.11 as 802.11i, the Wi-Fi Alliance created a certification known as WPA.

Their WPA2 certification is based on the ratified IEEE 802.11i document, and WPA was based on part of the 802.11i draft document available at an earlier time. Today, documents often refer to WPA and WPA2 as if they are the same thing, but there are differences. For example, WPA does not implement the Advanced Encryption Standard (AES) but WPA2 does.

However, both can be implemented using passphrases or authentication servers. When implemented with an authentication server, they are more secure, assuming a strong EAP type is used. One particular EAP type that was thought to be secure, but turned out to be very weak, was LEAP from Cisco. WPA2 is a mandatory feature for all new equipment that receives the WiFi Certification from the WiFi Alliance.

When using a passphrase and preshared key (PSK), to authenticate client STAs using WPA or WPA2, there is a known vulnerability. An attacker can listen for the four-way handshake that is involved in the WPA authentication process and use the CoWPAtty tool, as one example, to discover the passphrase.

If the attacker does not capture a four way handshake quickly, she can transmit a disassociation frame to the STA to force it to process the four way handshake again.

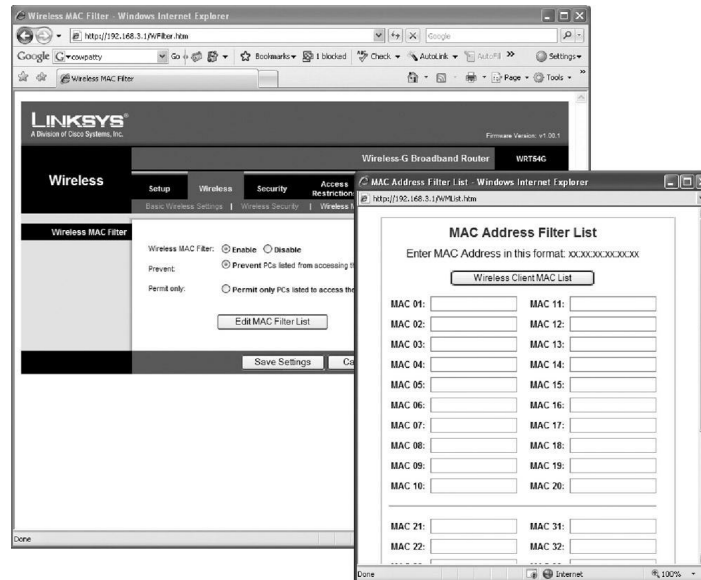
With the handshake frames, knowledge of the SSID, and a dictionary of possible passwords or passphrases, the attacker can eventually retrieve the passphrase and PSK. This type of attack is often called *WPA cracking*.

The primary protection against this attack, at this time, is to use enterprise-class security instead of the PSK. In other words, implement an EAP type that is secure, such as PEAP or EAP-TTLS, instead of using passphrases. You are likely to find yourself in an organization, if you install many WLANs, that cannot or will not support a full authentication infrastructure.

This usually happens in SOHO installations or SMBs. There are solutions to this like TinyPEAP, but in most cases, you can use a longer passphrase that is not a word at all (something like gu7YjhU67BbrYYZ89klop09) and gain enough security for these installations. According to some researchers, it could take years to bruteforce a passphrase like the one represented here even with a P4 3.8 GHz processor.

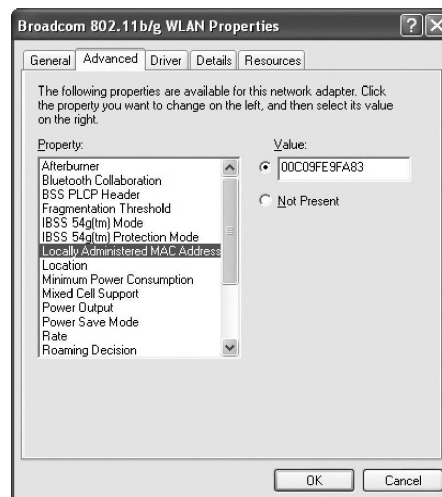
## **MAC Spoofing**

One of the earliest attempts at securing WLANs was to implement MAC address filtering. This simple technology involved including the list of MAC addresses that are allowed to authenticate with the AP or including the list of MAC addresses that are not allowed to authenticate. Below shows a typical configuration interface for this feature.

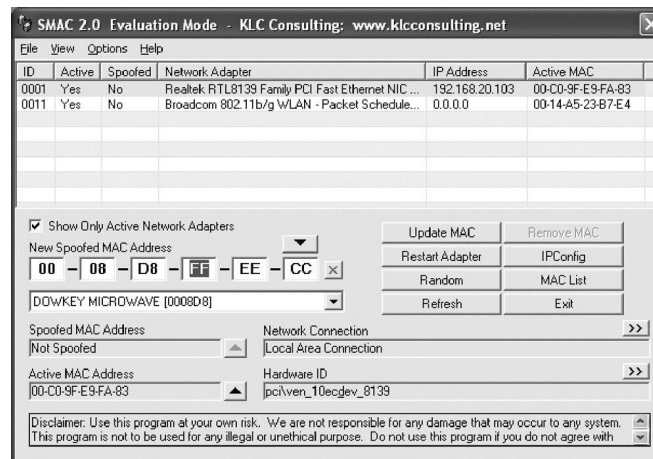


The feature is based on the fact that all IEEE 802.11 WLAN NICs have a physical address known as the MAC address. This address is either encoded into a NIC or is stored as a configuration parameter. The MAC address is normally read from hardware by the NIC device driver, but the device driver can be instructed to ignore what was read from the NIC hardware and to use a different address.

The problem is that, since many devices have a MAC that is specified as a configuration parameter, MAC addresses can be spoofed (faked or stolen). If an attacker can discover a valid MAC address, he can easily change the MAC address of his NIC to match. Below shows the Device Manager interface for changing a MAC address, which is available for many different WLAN devices.



In addition to the built in interface of many WLAN NICs, you can utilize applications like SMAC to change the MAC address of your WLAN card. SMAC works with almost any NIC, wired or wireless.



Using simple eavesdropping tools like CommView for Wi-Fi or OmniPeek Personal, an attacker can quickly determine the MAC address of users that are currently associated with your AP. If they are associated, their MAC addresses must be in the allowed list. All that the attacker has to do now is configure her MAC address and then authenticate and associate with the AP. This is why MAC filtering should not be considered a security solution at all. It may be considered a configuration enforcement solution of sorts, such as those described in [Chapter 7](#), but it should not be considered a security solution.

A common response to the reality of scenarios like this is "The attacker would have to have the right WLAN card to work with these eavesdropping tools, wouldn't he?" The answer is an affirmative one, but remember that attackers can pick up equipment at eBay now for very little cost.

## Peer-to-Peer Attacks

A *peer-to-peer attack* occurs anytime one WLAN STA attacks another WLAN station that is associated with the same AP. Hijacking attacks are sometimes referred to as peer-to-peer attacks as well.

These types of attacks must be protected against, as they are usually malicious. There is no real reason for an attacker to gain access to another peer computer other than theft or damage. Attackers may desire to penetrate your network in order to use it to gain access to the Internet. That is often their single intent. When an attacker tries to gain access to a client STA on your network, they are not likely to be doing it for Internet access.

Instead, they are likely to be performing a data theft or destruction attack. They may be attempting to install back doors into your network or other malicious software. Whatever their intention, it is seldom going to be benign.

To understand the potential severity of a peer-to-peer attack, consider the data that is often held on a user's laptop. Many users have personal information on their laptops as well as information belonging to the organization.

The personal information may include account names and passwords for online banking and other sensitive systems that the users access. The organization's information can include anything the users have read to access on the network.

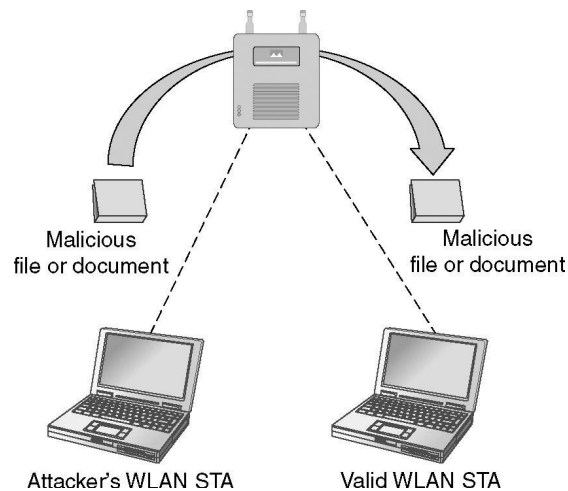
Users will often copy this information to the hard drive of their laptops so that they can view the information while traveling. Many times, the users are traveling through airports, which is just such a place where peer-to-peer attacks are likely to occur.

You can protect against these types of attacks using two common methods: endpoint security solutions or Public Secure Packet Forwarding (PSPF). Endpoint security involves the installation of an application on your WLAN STAs that monitors and reports on any attempts made by other STAs to access the monitored STA.

This kind of software may be bundled in with anti spyware or antivirus software. PSPF is a Cisco technology that allows you to disable access to WLAN client STAs by other STAs associated with the same AP or even the same ESS. Other vendors offer similar functionality, though they may call it by a different name. Below illustrates the concept of a peer-to-peer attack.

Notice that the malicious file is passing through the AP. This is normally the only way one STA can communicate with another in an infrastructure BSS. If STA-to-STA communications are disallowed, the attacker would have to perform a more complex hijacking hack to get the same malicious file onto the victim's STA.

An additional concern in peer-to-peer scenarios is the attacks that can occur in an ad hoc or IBSS network. In an ad hoc network, the users typically intend to share files with each other. For this reason and the fact that most computers today run Microsoft Windows, Windows file sharing is often enabled. This opens the door for attacks. In these types of ad hoc networks, the users should have firewall software installed (or more robust WLAN endpoint software, if it's available) and be trained in how to use it to limit the machines that can connect to their file shares and computer.



Another concern from the perspective of ad hoc networks is the common situation you find at airports and other public spaces. It is not at all uncommon to turn on your Windows-based laptop and select to "View Available Wireless Networks," only to find that there are dozens of ad hoc networks in existence.

Many of these, no doubt, are innocently configured machines with no ill intentions; but there can be no question that many of the ad hoc networks configured to have the identical SSID as that of the local airport or hotspot is there waiting for the unsuspecting user to connect so that the attacker can infiltrate the victim's machine.

These kinds of peer-to-peer attacks shed light on the importance of data classification procedures. *Data classification* can be defined as the process of labeling or organizing data in order to indicate the level of protection required for that data.

For example, you may define data classification levels of private, sensitive, and public. Private data would be data that should only be seen by the organization's employees and may only be seen by a select group of the organization's employees.

Sensitive data would be data that should only be seen by the organization's employees and approved external individuals. Public data would be data that can be viewed by anyone. For example, the information on the organization's Internet web site should fall in the classification of public data.

The contracts that exist between the organization and service providers or customers should fall in the classification of sensitive data. Finally, trade secrets or internal competitive processes should be classified as private data. This is just one example of data classification, but it help, you to determine which data users should be allowed to store off-line and which data should only be accessed while authenticated to the network. By keeping private data off of laptops, you help reduce the severity of a peer-to-peer attack that is launched solely to steal information.

## **Social Engineering**

*Social engineering* is a technique used for persuading people to give you something that they should not give you. Successful social engineering attacks occur because the target might be ignorant of the organization's information security policies or intimidated by an intruder's knowledge, expertise, or attitude.

Social engineering is one of the most dangerous and successful methods of hacking into any IT infrastructure—wired or wireless. Even in networks using more secure technologies like WPA-PSK as opposed to WEP, an attacker may be able to persuade an employee to reveal the passphrase that is being used.

Once the attacker has the passphrase, he will plug it into his own computer and wireless packet analyzers to view sensitive data in real time, just as though there were no security. For this reason, social engineering has the potential of rendering even the most sophisticated security solution useless.

Hackers (used in the negative sense of the term here) do not always fit the common profile of a technical recluse who is non sociable and unable to communicate well. Many times, the most successful and damaging network intrusion is accomplished in broad daylight through clever efforts of someone who walks into a business like he owns it.

In the very same manner, a hired professional security auditor should openly attempt intrusion as one tactic of testing security policy adherence.

There are some well-known targets for this type of attack:

- ◆ The Help Desk
- ◆ On-site contractors
- ◆ Employees (end users)

## The Help Desk

Because the Help Desk exists to provide help, it may become an easy target for a social engineering attack. The Help Desk employees are probably used to assisting internal employees with network configuration issues and WLAN access problems.

For this reason, they are probably well armed with information about how to configure a client computer to access the organization's WLAN. These professionals should be trained on what to give out and what not to give out over the phone.

There should also be some form of identity verification mechanism in place any time they do assist someone in gaining access to the WLAN. Items that might be marked as private and needing such identity verification are

- ◆ Hidden SSIDs of access points
- ◆ PSK passphrases, if used
- ◆ Physical locations of access points and bridges
- ◆ Usernames and passwords for network access and services (i.e., e-mail)

The auditor should (and the hacker *will*) use three particular tactics when dealing with Help Desk personnel:

- ◆ Forceful, yet professional language
- ◆ Playing dumb, afraid, or stressed (people like to help relieve other people's stress)
- ◆ Speaking the language of the organization (for example, if the technology group has a special name like *CompanyName* Information Services, be sure to use that terminology or, even better, the acronym for that term)

All of these approaches have the same effect: getting the requested information. Help Desk personnel understand that their job is to help people with their problems. They also understand that their manager will not be happy with them if their customers are not happy with the service they are receiving.

Many times, a threat to speak with, or write a letter to, the manager can help the social engineer to get the Help Desk person to give over the requested information just to appease and settle down the social engineer.

Playing dumb is a favorite of many social engineers. The Help Desk person is usually disarmed and stops paying attention when they figure out that the person to whom they are speaking knows very little. This situation is exacerbated when the "dumb" customer (the social engineer) is overly polite and thankful for the help. It's important that a Help Desk person be alert to this tactic at all times.

A social engineer is likely to call over and over, hoping to speak with different representatives, and taking different approaches with each.

When you speak the language of the organization, you fit in. If you do not, there is an almost subconscious awareness that something is wrong, and this may cause the victim to be on higher alert, which is exactly the opposite of what a social engineer wants.

## Contractors

A second group that the social engineer may target is that of temporary contractors. Contractors usually have no loyalty to the company in the first place, and this can lead to a more liberal handling of private company information. Sometimes, contractors are actually the individuals performing the network attack.

This was the case with Kevin Mitnick in many of his attacks in the 1990s. He was employed as a contractor and proceeded to attack the organization and steal proprietary knowledge, costing companies millions of dollars by some estimates. In many of these cases, he used social engineering methods to acquire the information. The fastest solution to the contractor dilemma is to be sure to give contractors only the level of access they need to get their jobs done and then train employees well in identifying social engineering or in protecting company interests.

However, because advanced social engineers are very skilled at their craft, you must consider that it is very likely that a user will give up valuable information to these individuals. Storage level encryption and intrusion prevention or monitoring systems may help in these scenarios.

### **Employees**

It is not uncommon to walk down the hallway of an organization and hear one employee loudly calling out his username and password to another employee in a different cubicle or work area. We tend to develop trust for people we work with on a regular basis, and this often causes us to take actions we really shouldn't take. High trust is a very good thing for productive work, but it can also lead to the sharing of sensitive information that should not be shared.

In the end, social engineering is a very powerful attack method that cannot be protected against by technologies alone. This attack method takes advantage of the ever-present human factor, and to protect against it, we must improve our humans and not just our technologies. Better training is required, and refresher training classes may also be needed. The good news is that you can usually provide the needed awareness training class in a 45- to 90-minute window once or twice a year. It can even be incorporated into annual employee meetings, but it must not be forgotten.

### **Know Your Enemy**

Over the years, there has been a fair amount of research on why crackers crack and the kinds of personalities that tend to become crackers. The reality is that the pool includes introverts and extraverts. It includes people who are in it for the money, the fame, and even the cause (whatever it might be). Because of this, I've chosen to look at the technical proficiency of the attacker rather than the emotional, social, or financial motivations of the attacker. By considering the technical proficiency, I can better organize my protection mechanisms to deal with the threats that I am most likely to face. The three categories I look at are the following:

- ◆ Wannabees
- ◆ Gonnabees
- ◆ Killerbees

The Wannabees are often called Script Kiddiez by the security community. This name has been associated with them because they cannot really crack a system; however, if they have stepbystep instructions, they can penetrate a system that has a known vulnerability.

In the preceding paragraph, we said that the Wannabees wouldn't likely breach my six character passphrase for WPA-PSK. The reason is simple. They are parked at the Stop sign in front of my house, and as soon as they see my network would require some effort, they go on to my neighbor's network that is wide open. These attackers are usually not malicious toward the specific network they are attacking. They will attack any network that has a known vulnerability.

There are cases where Wannabees perform intentional attacks against networks that represent philosophies or ideas to which they are opposed, but these attacks are the exception and not the rule.

Those that I categorize as Gonnabees are the crackers and hackers with a moderate to high level of skill. They may use a mix of instructions and existing knowledge, but they are much more dangerous than the Wannabees if they choose to use their skills for bad rather than good.

I would like to think that there are more Gonnabees on the side of obedience to the law than there are law breakers, but this is only wishful thinking, since there is no real way to track how these skilled crackers and hackers use their abilities.

To protect against this skill level, I will need to implement strong authentication and confidentiality.

The final level, the Killerbees, is the category of attackers who combine the technical proficiency of the Gonnabees with deep knowledge of human engineering. This allows them to become masters of social engineering as well as technical cracking. There is no more skillful foe. Enduser training and strong authentication and confidentiality will be needed, but greater measures will also need to be taken.

Continual awareness of changes in the environment will be necessary as well as frequent reeducation of the user community. This is more important in larger organizations that receive more media coverage and are therefore more likely to be targets of attacks at this level. Smaller organizations that are involved in markets that see strong resistance from various social groups must also be on the lookout.

Of course, regardless of the level of technical skills possessed by the attackers who threaten you, there are minimum security measures you should always employ. For example, intrusion monitoring and activity logging should always take place at some level. Regular updates to software and firmware is also a given.

Every organization should take measures to protect against the Wannabees. These individuals with little technical skill but a desire to penetrate networks and possibly cause damage abound. You can protect your network from these attackers using standard security precautions, which include:

- ◆ Using modern secure encryption technologies
- ◆ Patching computers and devices with updates to software and firmware
- ◆ Providing periodic awareness training to your end users
- ◆ Implementing effective authentication, authorization, and accounting procedures

To protect against the Gonnabees and Killerbees, you have to go a step further. Standard security practices will thwart many attack attempts by these advanced crackers, but you must implement stronger security mechanisms when applicable. You will determine applicability by balancing the value of your assets against the risk of attack.

For example, a small company that sells nuts and bolts has a much lower risk level than a small organization that exists in order to promote a social agenda. The former organization is involved in work that most people would consider trivial or non divisive.

The latter organization is more likely to be considered divisive and nontrivial. For this

reason, the latter organization is more likely to be attacked by both skilled and unskilled crackers. Most small organizations do not implement advanced intrusion prevention systems, but the latter organization in this case may need to implement just such a solution.

## General Security Principles

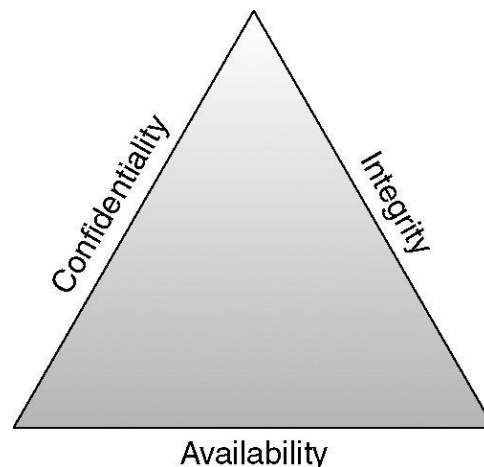
This chapter has introduced you to the wireless vulnerabilities and attack methods that are commonly executed against IEEE 802.11 networks. The [next chapter](#) will introduce you to the protection mechanisms that are available and will also expose a few more vulnerabilities.

I will end this chapter with a brief overview of two security concepts that are often referenced when dealing with computer security, network security, or internetwork security, which I will refer to as *information security* to encompass all three of these traditional terms. This will prepare you for the chapter that follows. The two concepts are:

- ◆ CIA
- ◆ AAA

### CIA

*CIA* stands for *confidentiality, integrity, and availability*. This acronym is often used to reference these three extremely important concepts in information security. They are sometimes called the *CIA security triad* or just the *CIA triad*.



*Confidentiality* is the concept of keeping private information private. It is accomplished by restricting access to the information when it is stored, transferred, or utilized in any other way.

During storage it is achieved by encrypting the data in some cases and restricting access to it in all cases. During transfer, it is achieved through the use of encryption. During utilization, it is achieved by means of physical security, which controls access to the area where the information is being used on screen or in print format.

An example of weak confidentiality is the WEP encryption in IEEE 802.11. *Integrity* is the concept of data consistency. In other words, the data is what it should be. This must be true when the data is transferred from one place to another.

For example, a man-in-the-middle attack may involve receiving data from an unsuspecting client and changing it in some way before it is sent to the destination. When this occurs, the data integrity has been violated.

This is usually protected against, through the utilization of hashing algorithms and CRC methods. A hijacking attack that evolves into a man-in-the-middle attack, then, is an example of an integrity violation.

*Availability* simply states that the right data is available to the right people at the right time in the right place. This is a factor of data throughput as much as it is of data security. However, if you've provided sufficient throughput and then an attacker performs a DoS attack, availability suffers. A DoS attack, then, is an example of a security breach that would violate the principle of availability.

These three concepts must be considered when implementing your WLAN. Not only must you consider how you will provide confidentiality, integrity, and availability, but you must also consider which is most important. For example, stronger encryption may require more overhead that in turn reduces availability (throughput).

The same is true for various integrity algorithms. If availability is highly important, you will have to either sacrifice the level of confidentiality and/or integrity or implement hardware that is powerful enough to overcome the overhead. This means that your WLAN will cost more, but it is often worth the cost.

## AAA

The second fundamental concept of information security is *authentication*, *authorization*, and *accounting* (or *auditing*), which is called the AAA (pronounced triple-A) in many references. Think of these three factors like this:

- ◆ *Authentication* Who are you?
- ◆ *Authorization* What do you want?
- ◆ *Accounting* What have you done?

If you remember these three simple questions, you'll always be able to remember these three important factors. As you can already see, without all three, I cannot really have accountability on my network. As a definition of accountability, consider the following:

Accountability is the concept that says all network users are responsible for the actions taken by their individual network accounts.

In other words, the users are responsible for protecting their accounts as well as the actions they take while connected to the network with those accounts. This is an important concept.

Without this concept of accountability, you have users sharing their authentication information with other users and you lose all accountability on the network. Of course, enforcement is another story completely different.

When you consider the three factors of AAA, authentication simply must come first. You must first verify the identity of an individual before you can grant him access to resources as an individual.

Authorization is the granting of access to resources. Since this is the case, strong authentication is essential to solid information security. If your authentication is weak, the trickle effect will be weak or irrelevant authorization and accounting.

If you authenticate users but do not utilize effective authorization (for example, you allow everyone to access everything), then your accounting will serve a much diminished purpose. The point of accounting or auditing is to track who does what and when they do it on your network. If everyone can do everything, users will be very slack in protecting their

credentials, and therefore, the entire AAA concept is weakened. As you can see, you need all three to have strong information security.

## **Summary**

In this chapter, you learned about the different WLAN attack methods that are common. You discovered some of the inherent weaknesses of WLANs, which is the first part of the journey to learning to secure them. In the process, you discovered how attackers can view the frames on your network, decrypt the traffic on your network, and hack the preshared keys used to authenticate to your network. You also learned how attackers can take over a user's computer and attack it or monitor the traffic going in and out of it. Now that you know how attackers attack you, you're ready to move on and learn how to protect against their attacks.

## Review Questions

1. You are the network administrator for an SMB located in West Virginia. The single AP your organization uses is configured with WPA–PSK, and the preshared key is set to your company name followed by the number 7. Is this a secure implementation and why?

- A. Yes. It is secure because WPA–PSK resolved the problems with WEP.
- B. Yes. It is secure because the preshared key is at least five characters long.
- C. No. Because it only includes the company name plus one digit, it could be easily guessed.
- D. No. Because WPA–PSK is just as insecure as WEP, it should never be used.

2. While performing a penetration test on a WLAN, you attempt to connect to the IP address of the AP in a web browser. Your connection is denied when connecting through the WLAN. What attack method is being protected against in this scenario?

- A. Denial of service
- B. Authentication cracking
- C. Encryption cracking
- D. Management interface exploits

3. An attacker starts a software–based AP on his laptop. He then scans for the SSID of the AP at the coffee shop hotspot where he is located. He sets his software–based AP to use the same SSID. What type of attack is he likely beginning? (Choose all that apply.)

- A. Hijacking
- B. Encryption cracking
- C. Man–in–the–middle
- D. Authentication cracking

4. You receive calls from five different users in a 10–minute window of time. Each of them tells you that the WLAN is no longer available. You connect to the IP address of the AP across the wired network and can connect with no problem. This reveals that the AP is still running fine. What kind of attack is likely to be occurring?

- A. Hijacking
- B. Encryption cracking
- C. Denial of service
- D. Management interface exploit

5. An attacker is preparing to perform an eavesdropping attack at a hotspot. Like most hotspots, this one uses no encryption, so the attacker knows she can view the data frames easily. She runs NetStumbler and determines that there are two APs providing coverage in her area. One is on channel 1, and the other is on channel 11. To which AP will she need to associate in order to launch the eavesdropping attack?

- A. Both
- B. The one on channel 1
- C. The one on channel 11
- D. Neither

## Answers

- 1. C.** When the passphrase includes the company name or some other easily guessed word or phrase and one digit, the entire phrase is easy to guess and does not provide adequate security.
- 2. D.** This scenario demonstrates the protection against management interface exploits. Attackers often attempt to connect to the IP address of the AP using a web browser in order to guess passwords to the web-based interface. If they can get in, they can take over the device.
- 3. A, C.** He is most likely beginning a hijacking or a man-in-the-middle attack because both of these attack methods usually begin by setting up a software-based AP.
- 4. C.** The most likely attack is a denial of service (DoS) attack. Since you can access the AP, it is not likely to be a Layer 2 management frame flooding attack. It is most likely an attack where a signal generator is in use at Layer 1.
- 5. D.** She will not need to associate with an AP in order to eavesdrop on the network. She can simply start her WLAN protocol analyzer and capture frames on channel 1 or 11.