Chapter 12

Wireless Security Project Plan

Solutions in this chapter:

- **Wireless Security Auditing**
- **Project Parameters**
- **Project Team**
- **Project Organization**
- **Project Work Breakdown Structure**
- **Project Risks and Mitigation Strategies**
- **Project Constraints and Assumptions**
- **Project Schedule and Budget**
- **Wireless Security Project Outline**

- ☑ **Summary**
- ☑ **Solutions Fast Track**

Introduction

In this chapter, we'll provide the framework for creating a wireless security project as part of your overall corporate IT security strategy. As with all the individual security area projects (ISAPs) discussed in this book, it is intended to be a template to use as a starting point. There is no one-size-fits-all project plan for any security topic, and wireless security is no exception. You will need to modify this project plan to fit your organizational needs in many different ways but you will find the basic building blocks here.

Wireless technology continues to evolve and so, too, do the tools hackers use to gain unauthorized access to wireless networks. Even as recently as two years ago, a majority of corporate wireless networks were unsecured, allowing anyone with a wireless card to access the network. In the past couple of years, more companies have begun securing their wireless networks in a variety of ways (though a surprising number are still unsecured). Some companies have created a separate wireless network for customers or guests that does not connect in any way to the corporate network (such as those often found in hotels, coffee shops, and airports). Other companies have applied basic security such as Wired Equivalent Privacy (WEP), which was once thought to be secure but has since been shown to be hackable; or Wi-Fi Protected Access (WPA), a stronger but more difficult-to-administer security solution for wireless. We won't get into the pros and cons of various wireless security solutions in this chapter, though we will discuss various technical elements and let you decide what will work best for your organization.

Even if your company does not have a wireless network, you still need to perform an audit because an intruder or employee can easily install a rogue wireless access point at just about any place on the wired network to provide unauthorized wireless access. So, don't think that because your IT department hasn't implemented a wireless network that others (inside and out) haven't already done so without your knowledge. The bottom line is this: wireless networks must be secured to meet the specific needs of *your* organization

and you must also be aware of all wireless access to the network. In this chapter, we'll get you started down that path.

In addition, a laptop with a wireless connection at an airport or hotel lobby accessing the corporate network via the Internet exposes your firm to the same wireless hazards as a corporate wireless network does, so you do need to have a wireless security plan for your organization.

Wireless Security Auditing

Before you can embark on just about any IT security project, you need to understand the current environment. In project management, as we've stated several times, you should start with a problem statement. The problem statement for wireless security can be as general as, "We don't have adequate security for our wireless network and corporate resources are at risk." However, the more specific you get, the better your solution will be. If you say, "We currently have 25 wireless access points (WAP) that are operating without security and we have no idea how many rogue WAPs we have," you are getting closer to defining the real problem and closer to identifying the real need. One way to develop a solid problem statement can be through auditing.

Auditing means different things to different people but we'll use a definition commonly used in the IT security world: a thorough and methodical review of systems and technologies focusing on finding vulnerabilities. Some companies hire outside security consultants to assist with their security auditing. If you choose to perform your own wireless security audit, you're going to need several tools to do so and you're also going to need to put on your "hacker's hat" so you can discover vulnerabilities hackers would likely exploit.

Hackers, like robbers or car thieves, will attack the easiest targets first. In the case of wireless networks, they'll certainly take an unsecured wireless network over a protected one any day. Although both WEP and WPA can be hacked, both require more time, effort, data, and sophistication to do so. Just like the car thief, the easiest car to steal is a car that is (in this order):

1. Running with the key in the ignition.
2. Unlocked.
3. Locked.
4. Locked and using a security device (e.g., a steering wheel lock).
5. Locked, with an alarm system.
6. Locked, with an alarm system and an engine-disabling device.

For a hacker, the easiest networks to hack are those that are unsecured. However, corporations can be pretty rich targets for hackers—either because of the presence of personal data on the network (credit cards, personal identification, etc.) or because they can access corporate trade secrets, R&D, and other confidential corporate data. Hackers will try to find a way in if they believe it's fun, interesting, or lucrative to do so. Finally, there is simply the hacker-of-convenience who hacks into a network just to see if he or she can. Therefore, your goal in wireless network auditing is to find the vulnerabilities from easiest to hardest (just like our car thief). If you plug the obvious holes, you're better off than doing nothing, but you're not secure.

Also keep in mind that there are a growing number of wireless devices, all of which you need to manage. Users with laptops, PDAs, smart phones, and other devices are accessing all kinds of information on the Internet, both from your corporate network and elsewhere. They're like little kids out playing at school—you have no idea what they may have gotten into and what kinds of viruses they may bring into the organization, all through relatively innocent activities. It doesn't really matter how secure your network is if traveling employees access confidential data across an unsecured link. These are the kinds of things you need to be aware of when you assess your wireless environment from end to end.

Business Intelligence…

Outside Consultants Sometimes Make Sense

Our goal is not to push you to use outside consultants, but to remind you that there are expert resources available to you. When it comes to security, you may just want to hire a specialist. Think of it this way: If you sprain your ankle or break your leg, you can go see just about any competent medical doctor for treatment, but if you have a leaking heart valve or some other more difficult medical problem, you want a specialist who has been down this path hundreds (if not thousands) of times. You want someone who knows this specialty cold, who brings his or her experience, expertise, and specialized training to your aid. The same is true of a security consultant who has solid credentials. He or she will know the common security holes, common errors made in corporate security, and the latest tools and techniques for assessing and tightening security. If you have this type of specialized expertise on your IT team, you're in great shape. If you don't, you may look to an outside consultant to help you audit your security (from a full network audit to individual security area audits) so you can develop the best security plan possible. Although an outside consultant might cost you more initially, it is likely that in most companies that cost will be quickly offset by a more thorough and reliable security audit report, shorter time to implement appropriate security solutions, and higher overall security. One caveat: Know what you're looking for before you sit through security consultant presentations. If possible, work with a firm you're familiar with or that comes highly recommended to you and always check references. You want to find the right firm for *your* company and *your* project, not the firm with the most persuasive sales team or the glitziest PowerPoint presentation.

Types of Wireless Network Components and Devices

There is a long list of actual devices that can be used in a variety of wireless environments. For now, let's look at the top-level categories. These include:

- Wireless Local Area Network (WLAN), including wireless access points (WAP), bridges, wireless keyboards, WLAN clients, or Wireless Personal Area Network (WPAN) Bluetooth clients
- Cellular phones with Internet capabilities or camera capabilities
- Radio Frequency Identification (RFID)
- Broadband wireless networks or cellular data interface cards (3G) in PDAs
- Two-way pagers and Short Messaging Service (SMS) devices
- Blackberry devices and Blackberry Enterprise Server

Wireless devices and technology are changing all the time and the wireless capabilities continue to expand, so be sure to take a look at the technological landscape at the time you plan your wireless security project to determine if the list provided should be expanded for your project. Table 12.1 also categorizes wireless devices by network connection, operating system, and how it participates in a wireless network. This may be helpful to you in looking across your organization at all wireless devices.

Table 12.1 Wireless Devices to Secure

Wireless Technology	Environment
Wireless network	Wireless Local Area Network (WLAN), Wireless Personal Area Network (WPAN), Wireless Wide Area Network (WWAN)
Radio Frequency Identification (RFID)	
Wireless camera	Wireless client, network device, embedded OS
Wireless access point (WAP)	Infrastructure, operating system, network access
WLAN Security gateway, router, bridge, or switch (functionality often imbedded with WAP)	Infrastructure, operating system, network access

Continued

Table 12.1 continued Wireless Devices to Secure

Wireless Technology	Environment
WLAN or WWAN (Broadband) Network Client (including laptops and other clients)	Wireless client, network device, operating system, applications, anti-virus, IP address
Personal Digital Assistant (PDA) with Network Interface Card (NIC)	Wireless client, network device, embedded OS, applications, IP address
PDA without NIC	Network device (via docking or sync station), embedded OS, applications, no IP address
Blackberry Enterprise Server	Wireless server, network (member) server, operating system, server application, anti-virus
Blackberry client devices	Wireless client, network device, embedded OS, applications
Wireless phone	Wireless client, network device, embedded OS
Wireless Voice over IP (VoIP) system and telephone devices	Embedded OS, wireless telecom
Wireless keyboards and mice	None

Adapted from "Wireless Security Checklist, Version 3, Release 1.3, 20 April 2006." Developed by Defense Information Systems Agency (DISA) for the Department of Defense (DOD).

If you're interested in reviewing the entire spectrum of security checklists available from DISA, visit the National Institute of Standards and Technology (NIST) Web site at http://csrc.nist.gov/pcig/cig.html. The checklists are written in a very specific format that may not be useful to you, but the information contained within the templates may be useful. They can be used as a starting point for creating a detailed security assessment or audit for a variety of topics including access control, Microsoft's Active Directory, biometrics, Cisco's IOS Router, and many more.

Wireless Technologies

Although it's important to be aware of the various kinds of wireless technologies, the primary focus is on the standard wireless networking components we're all pretty used to by now. Let's take a brief detour to understand the wireless standards.

The wireless standard issued by the Institute of Electrical and Electronic Engineers (IEEE) is known as IEEE 802.11. Here's a quick summary:

- **802.11** Has data speeds of up to 2 megabits per second (Mbps) and uses either Frequency Hopping Spread Spectrum (FHSS) or Direct-Sequence Spread Spectrum (DSSS) transmission techniques. Even though both are based in the ISM (Industrial, Scientific, and Medical) radio band, FHSS and DSSS devices cannot network with each other.
- **802.11a** Has data speeds of up to 54 Mbps and uses the Orthogonal Frequency Division Multiplexing (OFDM) technique in the U-NII (Unlicensed National Information Infrastructure) radio band.
- **802.11b** Has data speeds of up to 11 Mbps and uses only the DSSS technique in the ISM radio band. It's backward-compatible with 802.11 DSSS devices.
- **802.11g** Has data speeds of up to 54Mbps and uses both OFDM and DSSS techniques in the ISM radio band. Use of the DSSS allows it to be backward-compatible with 802.11b and 802.11 DSSS devices.
- **802.11n** This is the latest Wi-Fi standard but results aren't in yet. There are reports that there are interoperability problems so most consumers and businesses are taking a wait-and-see approach.

Although 802.11 debuted in the mid-1990s, wireless networking didn't become a big consumer item until the introduction of inexpensive 802.11b equipment in 2001. Even though the 802.11a standard was rati-

fied just prior to 802.11b, most manufacturers made "b" equipment first. 802.11a has a very short range in comparison to any of the other standards, due to the U-NII band, and has never gained much popularity. The subsequent standard, 802.11g, was ratified in 2003, and is backward-compatible with 802.11b and 802.11 DSSS equipment. For these reasons, 802.11b enjoys the most popular use, though 802.11g has caught up quickly. Next up, 802.11n. If you want to learn more about the standards, www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.std.html has some detailed information on how they came about. You can also read through the IEEE standards; they're located at http://standards.ieee.org/wireless. Another good resource is http://www.netstumbler.com.

Types of Threats

There are three primary categories of threats we'll discuss in this chapter: War dialing, war driving, and Bluetooth attacks. In a moment, we'll look at each one in detail. The majority of this chapter will be devoted to "traditional" wireless security—meaning the wireless networks created by wireless network interface cards and wireless access points connected to a wired network. This is where the bulk of the risk comes from in any company and therefore it should be the place where most attention is placed (from a wireless security perspective). However, there are several other types of attacks that fall within the "wireless" realm that should be understood and assessed in your network. Most of these "alternate" connection types can be quickly and easily located and secured, but the point is that you must be thorough in your wireless assessment so you don't overlook these easily secured openings. We'll begin by looking at attack methods from oldest to newest. *War dialing* started back in the days when remote computers communicated with one another only via modems over the public telephone systems. *Wardriving* is the updated version of that and uses wireless technologies rather than phone lines. Bluetooth, a short-wave radio signal communication method, also has its perils.

War Dialing, Demon Dialing, Carrier Signal Scanning

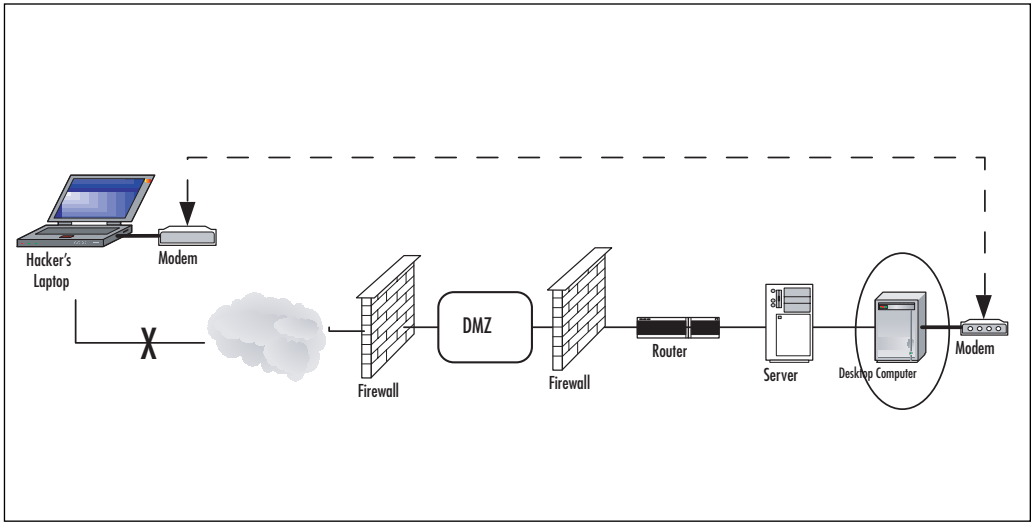
Although war dialing (a.k.a. demon dialing or carrier signal scanning) is not technically a wireless technology, it belongs in this arena due to the nature of the attack. *War dialing*, for those of you not familiar with this attack type, is when hackers dial phone numbers looking for misconfigured or unsecured modems. Remember modems? Many desktop computers and even many servers have modems sitting in them, even if they are unused and getting dusty in a virtual sense. War dialing can yield unexpectedly large rewards for hackers since modems are often forgotten elements and are therefore overlooked as part of a risk assessment or security monitoring project.

In a standard network configuration, all incoming traffic is routed through an external firewall and/or a perimeter network along with an internal firewall. However, with a modem in the mix, a hacker can essentially bypass all those layers of protection and go directly into the computer or server with the modem installed. The modem in and of itself is not a problem but because it may not be secured, it may create a security hole that you're not even looking for. You should take an inventory of all computers in your network to determine if they have modems and if they have phone lines connected to them. A modem by itself can't be utilized unless it's connected to a phone line, and some companies' phone systems don't connect well with standard RJ-11 jack types, so this may not be an issue for you. However, it never hurts to look. For example, if your company used to use modems, are you sure you're no longer paying for those modem lines from the phone company? Many corporate phone bills go directly to finance, not to the IT department, so it's entirely possible you have active phone lines that users might still be connected to (or that they could connect to). For example, if a corporate computer is configured with Symantec's pcAnywhere without username and password required, it's a wide open door for anyone looking to circumvent network firewalls and security measures, as shown in Figure 12.1. A hacker can easily bypass all the well-designed security systems and get right in an

open backdoor without any security measures at all. It doesn't take any very sophisticated tools or techniques to do this.

Keep in mind that if your company is still running legacy systems or components, many require the use of modems for maintenance and support activities. If these systems are connected to the network, they are part of your security environment. One of the best ways to secure these types of systems is to enable the dial-back feature so that an incoming call is disconnected and the call is returned to a specified phone number.

Figure 12.1 Network Exposed Via Modem



Business Intelligence…

The Art of War Dialing

Peter Shipley and Simpson Garfinkel wrote a document called "An Analysis of Dial-Up Modems and Vulnerabilities" in 2001 (http://www.dis.org/filez/Wardial_ShipleyGarfinkel.pdf). They used an automated process to dial over 5.7 million phone numbers looking for

Continued

unsecured modems in the San Francisco area. Although the method they used was dialing blocks of numbers within area codes, an easier way is to dial blocks of numbers associated with a business's main phone number. If your company's phone number is 555-1000, a war dialer would dial every number between 555-1000 and 555-9999 looking for a modem. Of the 5.7 million numbers Shipley and Garfinkel called, 49,192 modems respond. What they found was that many of these modems were connected not just to open dial-up lines, but directly to application servers. Even though that was five years ago, the emphasis on high-speed Internet connections via cable modems, broadband, and T1 lines has left little attention focused on these "legacy" devices. A well-publicized event cited by these authors was a teenager who stumbled upon a dial-up line and was never asked for a username or password. With open access, he was presented with various commands he could use, so he began experimenting. According to the article, the result was that the teen managed to shut down power to a regional airport and 600 nearby houses. Even though the teen was really just monkeying around, his rather innocent exploration had a major impact. The lesson—don't overlook modems as part of your security patrol. For the full story, check out the full article by Peter Shipley and Simpson Garfinkel at the link provided; it's a fascinating read and will open your eyes to a lot of security issues, not just war dialing techniques.

Wardriving, NetStumbling, or Stumbling

Wardriving is a term many IT people are familiar with—the term is a take off on the original term *war dialing* (based on a 1980s movie starring Mathew Broderick called *War Games*) and involves actually driving around in a car with a good antenna looking for unsecured wireless networks. Before we jump to any rash conclusions, however, let's hear what security experts have to say about *war driving*. This is an excerpt from *WarDriving: Drive, Detect, Defend: A Guide To Wireless Security* (Chris Hurley, Frank Thornton, Michael Puchol, and Russ Rogers, Syngress Publishing, Inc. 2004).

> These days, you might hear people confuse the terminology *WarDriver* and *hacker*. As you probably know, the term hacker was originally used to describe a person that was

able to modify a computer (often in a way unintended by its manufacturer) to suit his or her own purposes. However, over time, owing to the confusion of the masses and consistent media abuse, the term *hacker* is now commonly used to describe a criminal; someone that accesses a computer or network without the authorization of the owner. (If you choose to hack or modify your own computer, you're not engaging in a criminal activity.) The same situation can be applied to the term WarDriver. WarDriver has been misused to describe someone that accesses wireless networks without authorization from the owner. An individual that accesses a computer system, wired or wireless, without authorization is a criminal. Criminality has nothing to do with either hacking or WarDriving.

The news media, in an effort to generate ratings and increase viewership, has sensationalized WarDriving. Almost every local television news outlet has done a story on "wireless hackers armed with laptops" or "drive-by hackers" that are reading your e-mail or using your wireless network to surf the Web. These stories are geared to propagate Fear, Uncertainty, and Doubt (FUD). FUD stories usually take a small risk, and attempt to elevate the seriousness of the situation in the minds of their audience. Stories that prey on fear are good for ratings, but don't always depict an activity accurately.

An unfortunate side effect of these stories has been that the reporters invariably ask the "WarDriver" to gather information that is being transmitted across a wireless network so that the "victim" can be shown their personal information that was collected. Again, this has nothing to do with WarDriving and while a case can be made that this activity (known as *sniffing*) in and of itself is not illegal, it is at a minimum unethical and is not a practice that WarDrivers engage in.

These stories also tend to focus on gimmicky aspects of WarDriving such as the directional antenna that can be made using a Pringles can. While a functional antenna can be made from Pringles cans, coffee cans, soup cans, or pretty much anything cylindrical and hollow, the reality is that very few (if any) WarDrivers actually use these for WarDriving. Many of them have made these antennas in an attempt to both verify the original concept and improve upon it in some instances.

The reality of WarDriving is simple. Computer security professionals, hobbyists, and others are generally interested in providing information to the public about security vulnerabilities that are present with "out of the box" configurations of wireless access points. Wireless access points that can be purchased at a local electronics or computer store are not geared toward security. They are designed so that a person with little or no understanding of networking can purchase a wireless access point, and with little or no outside help, set it up and begin using it. Computers have become a staple of everyday life. Technology that makes using computers easier and more fun needs to be available to everyone. Companies such as Linksys and D-Link have been very successful at making these new technologies easy for end users to set up and begin using. To do otherwise would alienate a large part of their target market.

The Legality of WarDriving

According to the FBI, it is not illegal to scan access points, but once a theft of service, denial of service, or theft of information occurs, then it becomes a federal violation through 18USC 1030 (www.usdoj.gov/criminal/cybercrime/1030_new.html). While this is good, general information, any questions about the legality of a specific act in the United States should be posed directly to either the local FBI field office, a cyber crime attorney, or the U.S. Attorney's office. This information only applies to the United States.

> WarDrivers are encouraged to investigate the local laws where they live to ensure that they aren't inadvertently violating the law. Understanding the distinction between "scanning" or identifying wireless access points and actually using the access point is the difference between WarDriving, a legal activity, and theft, an obviously illegal activity.

One of the more commonly used tools for wireless network detection is *NetStumbler*, which was created by Marius Milner and released in May of 2001. There is a PocketPC version of this program called *MiniStumbler*. As a result of the ease-of-use of this program and the proliferation of its use, many now refer to the activity of wireless network detection not as *wardriving* but as *netstumbling*, or simply *stumbling*. Since it is often an activity done with no malice whatsoever, stumbling certainly is more representative of what most people do with these programs.

Clearly, the downside to the proliferation of easy-to-use wireless components is that they come with no security configured right out of the box. More recent releases of the Microsoft operating system come locked down, by default, but earlier versions had been set to "open" by default and the system administrator had to lock down anything he or she didn't want open, on, installed, or available. Now, the operating system takes just the opposite approach—things are locked down, disabled, and not installed by default, and the system administrator has to make a conscious effort to open things up. This approach is much better for network and server security but certainly doesn't encourage first-time users to give it a whirl. The balance between encouraging users and providing security is a delicate one, and most user-grade component companies like Linksys and D-Link are focused on the home user. As such, their equipment comes ready to install and use out of the box. Does that mean your home wireless network is at risk? Absolutely. Does it mean someone is going to come and steal your personal data? Who knows? If you live in a rural area, the likelihood of someone getting close enough for long enough to steal data is unlikely but certainly possible. If you live in an urban area, the risk obviously climbs because your neighbor in the downstairs apartment might be sitting there watching all your unsecured network traffic go by. However,

to go back to the comments made by the WarDriving experts, the real issue is that WarDriving itself is not an illegal activity and someone who uses your open wireless network may be unethically using your network, but if he or she does nothing harmful, it's a bit like running an extension cord to your neighbor's house to run your television set—it *is* stealing but it does not damage your television in any way. We're not here to support stealing unsecured wireless access, but to help you understand that not everyone who engages in wardriving has ill intentions.

If you perform a Web search for images using the search phrase "war driving maps," you'll find thousands of access point maps out on the Internet. Some sites keep up-to-date maps in a database, other sites are abandoned or outdated, but the overall impression you should get is that there are thousands of people looking for unsecured access points everyday for all kinds of reasons, and if you think your corporate wireless network or your wireless users are safe, think again. Figure 12.2 shows a sample map of the Los Angeles area.

Figure 12.2 Wardriving Map of Los Angeles, California

Source: http://www.cybergeography.org/atlas/wireless.html, Frank Keeney.

You can see that wireless networks are clustered, and anyone looking for wireless access could take a nice slow drive down Wilshire Blvd. or find a comfy coffee shop and take a look at tons of unsecured network traffic. The point is not to feed into the fear factor but to help you understand the reality of wardriving and the need to secure your corporate network and wireless users' wireless devices so that your network assets remain secure against the bad guys and the good guys who might accidentally stumble in.

Business Intelligence…

Wardriving for Fun and Profit

If you pay attention to what's happening in the outside world, you'll notice there's been a proliferation of information about wardriving in the past few years. At first, it was a subversive, secret underground world (or so it seemed), but these days there are many people who view wardriving as cheap entertainment—well not so cheap with the price of gas these days, but still very affordable. The tools and techniques are readily available for anyone seeking them. A laptop with a wireless card, a small fairly inexpensive antenna, and a tank of gas will get you started. If you're really strapped, you could do this on foot (some do in urban areas) with a well-equipped PDA (see Figure 12.3). Wardriving itself is not illegal when it's done simply to find and map secured and unsecured wireless access points (fun). Wardriving that leads to using someone else's unprotected network or network intrusion (profit) is illegal. Stumbling = ok, intrusion = not ok. It's a simple rule to follow for most.

There are thousands of Web sites that discuss wardriving and wardriving adventures. One that comes up in a search engine search is http://www.unwiredadventures.com, though there are many out there. On this particular site, the wardriver talks about his adventures in wardriving while vacationing with his family. This is a leisure activity he engages in to map wireless access points in various locations. Think of it as local geography with a twist. This excerpt from his Web site indicates his intention (from 2001): "Our trip was fun for all of us. Lots of good food and fun with our relatives. The kids were well behaved in the car

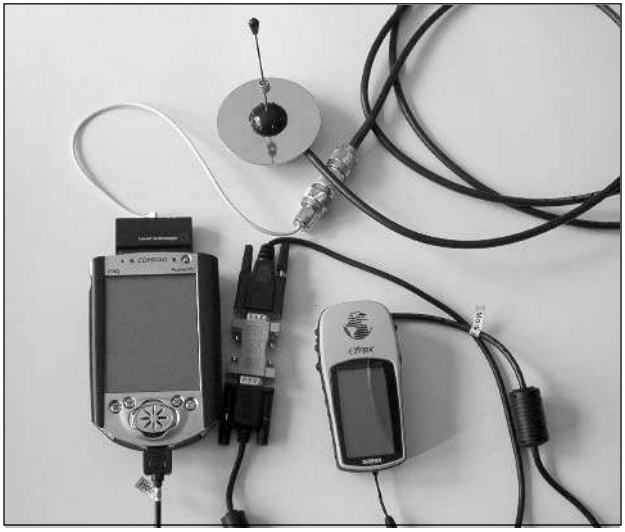
Continued

and my wife was understanding about the extra equipment in the car. 802.11b wireless equipment is very easy to install and has become very inexpensive. It's everywhere now, in homes and businesses. Wireless network technology has made the use of computer systems so very easy and convenient. Let's be sure to understand the equipment that we plug into our networks. Read the manuals, or hire an experienced security consultant to make sure that you are secure in your use of this technology." He mentioned that he has TCP/IP disabled on the computer he uses for wardriving so that he cannot inadvertently gain unauthorized access to corporate networks, though he admits that "Otherwise, it would have been easy to get free Internet access behind many corporate firewalls. Nearly all of the 802.11b wireless equipment that I have evaluated is factory configured with the lowest possible security settings. No access control and no encryption. It's up to the user to secure the equipment that is plugged into their network."

http://www.unwiredadventures.com/unwire/2005/12/vacation_war_dr.html.

A word to the wise: If you decide to give wardriving a try to hone your own skills, be sure to disable the TCP/IP stack on your wardriving device before you head out. This will prevent accidental intrusion to an unsecured network and keep you on the right side of the law.

Figure 12.3 Well-Equipped PDA for WarDriving



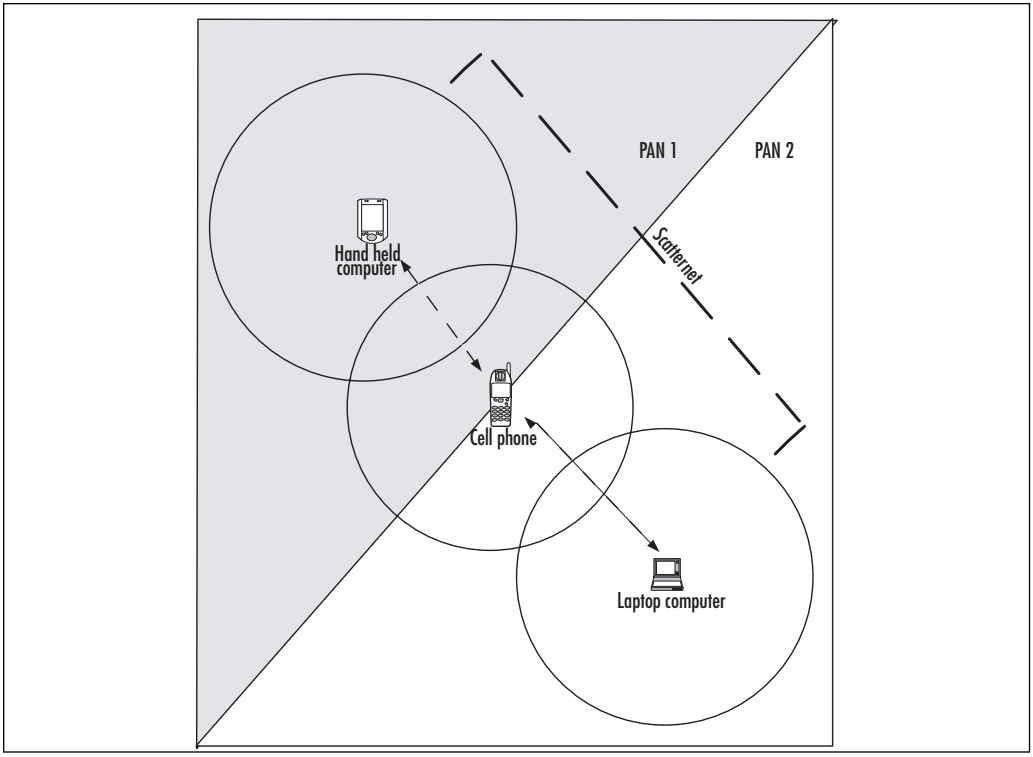
Some critics get upset by the proliferation of information available on how to set up equipment for wardriving. This is true for just about every computer activity that can be used for good or evil. E-mail communication is not a bad thing, phishing is. They both use the same tool (e-mail) for different purposes. The same is true of wardriving. The activity can be done innocently for fun or to hone technical skills, or it can be done to gather information in advance of an attack. Many in the security world are frustrated by the easy access people have to sniff, attack, and hack, but most also grudgingly agree that the more information that's out there, the more tools one has to understand and prevent unauthorized access. It's a never-ending cycle and you and your IT project team need to be on top of the latest tools, techniques, and tips that hackers have available so that you can secure your network—wired and wireless—from unauthorized access and harmful activities. We'll discuss the tools of the trade later in this chapter when we look at risk assessment for your wireless security project.

Bluetooth Attacks

As you probably know, Bluetooth uses a short-range radio signal to provide wireless communications, typically between various personal communication devices such as cell phones and headsets or PDAs. Bluetooth allows you to create a wireless personal area network (WPAN) that can communicate with other Bluetooth devices within a small physical radius (about 10 meters). Bluetooth relies on the use of radio waves and overcomes earlier infrared (IR) technologies that were used for personal communication devices. IR required line-of-sight for communicating with another device and it was a one-to-one connection. Bluetooth overcomes these limitations because it does not require line-of-sight and it allows many devices to communicate simultaneously. Bluetooth limits interference with other radio signals and other Bluetooth devices by limiting its broadcast range to 10 meters and by using a random frequency hopping algorithm. If interference does occur, it would be extremely short-lived since frequency hopping involves changing frequency several times per second.

Let's take a short side-trip to understand how Bluetooth devices communicate with one another so you can better understand the threat. Bluetooth devices "pair up" by exchanging a passkey (depending on the type and level of authentication selected). Once this occurs, the devices have essentially created a personal area network (PAN) in which one of the devices assumes the lead role ("master"). A single device can participate in multiple PANs, creating a *scatternet*, as shown in Figure 12.4. PAN1 and PAN2 form the scatternet and by design, the hand-held computer could be communicating, via the cell phone with the laptop computer. Since radio signals move through walls, the scatternet can be formed much like a standard wireless network. Some Bluetooth users mistakenly believe that their devices are safe but if you have Bluetooth enabled and you're not actively using it, it's possible your device is part of a scatternet without even knowing it.

Figure 12.4 Bluetooth Devices Forming a Scatternet



Business Intelligence…

The Art of Bluejacking and Bluesnarfing

Bluejacking first showed up in popular use in 2003 or so when Bluetooth devices gained popularity. Bluejacking is more of a prank than an attack, and an annoying one at that. The term apparently was coined in late 2002 by a fellow going by the moniker *ajack*. Although there are some rather amusing stories about bluejacking, to date there are no stories of unmitigated corporate network attacks having their genesis in a bluejacking. A story in 2003 by the Associated Press is a great example of how bluejacking typically works.

"The group of lanky tourists strolling through Stockholm's old town never knew what hit them. As they admired Swedish handicrafts in a storefront window, one of their cell phones chirped with an anonymous note: "Try the blue sweaters. They keep you warm in the winter." The tourist was "**bluejacked**" — surreptitiously surprised with a text message sent using a short-range wireless technology called Bluetooth. As more people get Bluetooth-enabled cell phones — both sender and recipient need them for this to work — there is bound to be more mischievous messaging of the unsuspecting. It's a growing fad, this fun with wireless. Already, Web sites are offering tips on **bluejacking**, and collections of startled reactions are popping up on the Internet." —Matt Moore, "Cell phone messaging takes a mischievous turn," *The Associated Press*, November 13, 2003 (from http://www.wordspy.com/words/bluejacking.asp).

Bluesnarfing, on the other hand, is an illegal activity that involves stealing data from a Bluetooth-enabled device. Typically, this involves stealing contacts or calendar entries. The calendar entries might be embarrassing ("Cosmetic surgery, 4 pm") but rarely damaging unless the calendar entry also has confidential information in it ("Meet Doug M. at 2 am in southwest corner of parking lot to hand off illegally gotten trade secrets"). More importantly, most of us don't want our contacts just handed over to a complete stranger. If you're like most people, you have a mixture of personal contacts (Mom, Dentist, Local Pizza Place) and business contacts (Boss: Home, Boss: Work, Boss: Cell, Boss: Husband, Boss: VacationHome, CEO of Company A, CIO of Company B). It would

Continued

be pretty creepy (and potentially dangerous) to have your mother get phone calls at 2 am from someone telling her that he knows her home phone number, address, zip code, and alarm code.

Stealing calendar and contact information via bluesnarfing requires both Bluetooth devices be on and available. The quickest and easiest way to avoid bluesnarfing (which requires about two to three minutes of continuous connection time) is to disable Bluetooth when not specifically in use. If you're using a cell phone with a Bluetooth headset, you can disable *Discovery* mode (sometimes called Visible mode), which makes it difficult for someone to find your Bluetooth-enabled device.

There's an excellent article you can read from 2004 that contains in-depth information about various Bluetooth attacks and the devices that were (at that time) vulnerable to such attacks. Head to this URL for more information: http://www.thebunker.net/security/bluetooth.htm.

One might argue that the threats to Bluetooth devices are greatly exaggerated by the media. At the same time, if you're sitting in a crowded airport awaiting your flight, there's always a chance someone could grab your contacts and have a field day with them. Suppose you were fortunate enough to get the home phone number (or the private line at the remote cabin) for the CIO of your company, a Fortune 500, publicly traded company. Do you really want someone getting that number, calling the CIO in the middle of the night saying that the Director of IT Security (you) gave the caller his number? Talk about a CTM (*Career Terminating Move*). The point is that confidential information is routinely stored on Bluetooth devices from PDAs to cell phones and data is at risk, regardless of how great or small you perceive that risk to be. This is an excellent example of a case where evaluating risk and remediation is pretty simple. You'll most likely create a user policy guideline (see the chapter on security policy later in this book) that requires users to set their Bluetooth devices so they are not in *Discovery* or *Visible* mode except when purposely participating in a Bluetooth network in a relatively safe location (at a business meeting, for example). Most (if not all) newer Bluetooth devices are updated to protect against attack but attackers are often smart, persistent folks and they'll no doubt find the

next open door to go through. Staying up to date on attack types is a never-ending task, so make sure there are people on your IT staff that are specifically tasked with doing so and keeping the rest of the team informed. Dividing this work into topic areas is a good way to keep everyone on the prowl for the latest data, and can be a great way to improve the skills of everyone on your team.

Risk Assessment

We know there is a trade-off between total security and total risk. There are financial and operational trade-offs that every organization must make. In the risk assessment phase of your audit, you need to look at your risks in terms of CIA: *confidentiality*, *integrity*, and *availability*. Data that is accessed wirelessly is most at risk of loss of confidentiality because it's relatively easy for a hacker to jump into the middle of an unsecured wireless stream and grab any data desired. However, he or she could also modify data (integrity) or simply make that data, network, or service unavailable, if desired.

Other key components of the wireless risk assessment are the *people*, *process*, and *technology* components. We'll talk about creating security policies for the organization in Chapter 13, which are used to help dictate and guide people's behaviors. *People* are almost always the weakest link in the security chain and your risk assessment should look at the risks people's behaviors (intentional and unintentional) have on security in the wireless realm. *Processes* must be assessed for risk as well. How do wireless users connect on-site? How do wireless users connect off-site? How should guest accounts be handled for wireless connections? There are a variety of process issues that should be assessed from end-to-end. Finally, the *technology* assessment should include an assessment of various wireless technologies in use along with the strengths and weaknesses of each. You also need to understand the technology available to the hackers and determine how to secure your wireless connections in light of hacker capabilities. Let's look at an example. It is possible to crack WEP encryption if a hacker has enough time, a powerful enough computer, and

enough data to do so. Therefore, WEP is usually sufficient for home wireless networks because a hacker rarely will be able to gather enough data in a short enough time frame to crack WEP on a home network and because there usually isn't a big enough pot of gold at the other end to entice a hacker to work that hard to break WEP on a home network (except in cases where there is targeted malicious intent or utter boredom). Contrast that to a corporate network where financial data including customer credit cards or bank account numbers or whatever are stored. Now there's a big enough payoff to make the time and effort worthwhile. So, you have to choose your battles and understand the relative attack footprint of your organization to understand where and how to secure your assets. That said, wireless is just a ridiculously easy target and you should take stronger precautions here than you might have otherwise considered necessary.

Remember, too, that there is no magic bullet. Wireless networking cannot be secured with 100 percent confidence. Security is often a matter of applying layers of protection to create a maze of problems most attackers will walk away from. A smart determined attacker with the right tools and enough time can probably crack anything, including the once-sacred WPA security. However, if you use MAC address filtering, you suppress SSID broadcasting, you use WEP or WPA and you educate your users, you've done all you can do. The rest is a matter of intelligently installing, configuring, maintaining, and monitoring an intrusion detection system and performing regular scans to make sure no ad hoc networks pop up.

Although we talked about risk assessment in Chapter 10, it's worth walking through a few of the risks inherent in a wireless network environment. There is some overlap but we will keep an eye focused specifically on wireless risks.

Asset Protection

As we have continually stressed, you have to find the right balance between protecting corporate assets and the cost of doing so. In any network assessment scenario, you should begin by understanding what you're

trying to protect and why. You may have addressed this issue adequately during your overall IT corporate security planning process. If so, you should review the data, assumptions, and outcomes at this stage to ensure your conclusions are still relevant and correct. Things change so quickly in most corporate environments that a quick review of previous assessment data is almost always a good use of your time. You should review what data is on your corporate network and what needs to be protected. This is also a good time to find out what is on your corporate network that perhaps should not be. If you recall the case studies from Chapter 1, it's not uncommon for corporate networks to have data on it that should not be there, such as credit card numbers or social security numbers that were stored inappropriately and in violation of corporate policy or vendor policy (as was the case with the credit card processing company, which violated its own policies and that of the credit card companies for whom they processed data).

In addition to discovering what is on your network (and what's there but shouldn't be), you also need to assess the relative value of that data. Though it can be argued that all corporate data is valuable, some data is clearly more valuable than other types of data. Remember that you need to think like a hacker to make these assessments. If all you have are lists of nuts, bolts, and cable lengths, there's not as much value to that data as there is with personal data such as credit card numbers, social security numbers, or bank access codes. Correlate the data on your network with the perceived value of the data to an outsider to understand the relative risk to your network. This will help you determine just how much security is appropriate for your specific situation.

A good example of this is a home wireless network. Most people using home wireless networks do not secure them even though they may log onto their online brokerage account or do some online shopping using a credit card. This data is transmitted in an unsecured manner from their laptop or wireless device to their wireless access point, then to the router or cable modem and then out to the Internet. Even if the Web site they are using is secured using SSL or HTTPS (for example), the link between the user's wireless device and the wireless access point may not

be secured. This is the weak link in this transaction. The same holds true of a corporate user at a coffee shop, hotel, or airport waiting area.

The question is this: how likely is it that a hacker is going to grab that data? Well, if you are in a dense setting where a hacker can sit in a nearby location and peruse wireless data like yours, then the *potential* is extremely high but the *likelihood* is somewhere in the mid-range on the risk scale. If you live in a more suburban or rural setting or are in a remote location of any kind where it would be difficult for someone to get close enough to receive your wireless signal, the risk drops significantly. The *potential* drops to low and the *likelihood* drops to near zero. Looking at the risk/reward proposition from a hacker's perspective will help you assess the relative value of your assets and what level of protection is warranted.

Sensitive Data

Sensitive data is defined differently from one company to the next. What's sensitive at one company may not be particularly sensitive at another. However, in most companies, there are clearly segments of data that are sensitive and your security audit should identify those areas. As part of your wireless security project definition stage, you need to clearly understand what data can be accessed via the wireless network (typically the connection in a corporate setting is to the wired network) and how sensitive that data is. It goes beyond the legal implications and into the business aspects. Lists of customers, vendors, suppliers, or employees can be sensitive, especially if you're in a medical setting, for example. Trade secrets, formulas, and research and development (R&D) data can be extremely sensitive, especially in industries that are working in leading edge or ground-breaking areas. This is a great place to get feedback and input from various departments in your company. Ask them what data they work with that they would not want posted on a Web site or printed in a newspaper. That usually gets people's attention and helps them begin to look at the data they work with on a daily basis from a slightly different perspective.

Sensitive data can be stored in a variety of locations, most notably (and insecurely) on laptops that leave the building. Employees could

intentionally boost sensitive data and if they are legitimate users of that information, it would be hard to know if they're doing something wrong. However, you also need to look at the possibility that users will transmit sensitive data via wireless laptop connections or that these laptops themselves might be stolen. In the chapter on operational security, we'll talk about physical laptop security, but for now, let's focus on laptops containing sensitive data that users transmit across unsecured wireless connections. Here's a quick list of data typically considered sensitive:

- Customer databases
- Employee lists
- Identity information (can include customer, employee, vendor)
- Credit card or other financial data
- Health information
- Intellectual property
- Trade secrets
- Research and development

Network Assets

In addition to data assets that hackers might target, there is another type of data that is often sought out by hackers and that is network data. If a hacker can get into the network using an unsecured wireless access point (or by any unsecured means, really), he or she will try to enumerate the network assets to find out where servers, databases, and sensitive information are located. Therefore, understanding the network configuration is often not the end-game but the intermediate step toward the final target. If you can prevent a hacker from gaining access to this network configuration data, you may prevent an intrusion. Network data that is helpful to a hacker includes (but certainly is not limited to):

- Usernames and passwords
- Directory listings

- Network firewalls, routers, switches, and hubs
- Network segmentation, including DMZs
- IP addresses for servers
- Ports and protocols in use

Business Intelligence…

The Cost of Identity Theft

The growing focus on IT security in all realms is because there is a growing problem with data theft—both corporate and personal. Companies must secure personal information but consumers must also do their part. There are 10 million identity theft victims in the United States each year. The average ID theft victim spends over 175 hours trying to fix the damage done and at a cost of over $1500 per incident. The total annual cost in the United States attributed to identity theft tops $15 billion. There are four basic types of identity theft:

- **Financial ID Theft**—This type of case typically focuses on your name and Social Security number (SSN). This person may apply for telephone service, credit cards or loans, buy merchandise, lease cars or apartments.
- **Criminal ID Theft**—The imposter in this crime provides the victim's information instead of his or her own when stopped by law enforcement. Eventually when the warrant for arrest is issued it is in the name of the person issued the citation—yours.
- **Identity Cloning**—In this crime, the imposter uses the victim's information to establish a new life. They work and live as you. Examples: Illegal aliens, criminals avoiding warrants, people hiding from abusive situations, or becoming a "new person" to leave behind a poor work and financial history.
- **Business or Commercial Identity Theft**—Businesses are also victims of identity theft. Typically the perpetrator gets credit

Continued

cards or checking accounts in the name of the business. The business finds out when unhappy suppliers send collection notices or their business rating score is affected.

Tips for businesses from the ID Theft Center include:

- **Information acquisition**—Do you need the information? Are you acquiring it in a safe manner?
- **Storage**—What computer security measures have you placed around the systems storing personal data? It should be considered highly classified and not common access.
- **Access**—Who has access? Is it on a need to know basis and access audited? Is there password control over systems? Is there a cafeteria worker asking your child for his/her SSN prior to receiving lunch? Did you do a background check on those who have access to personal information of employees and customers? Do temps have access to secure info?
- **Disposal**—Are electronic and paper documents containing personal information rendered unreadable prior to disposal? What is in your dumpster? Is it a treasure chest for thieves and for consumer action attorneys ready to sue you for placing their clients in jeopardy?
- **Distribution**—How do you handle information? Is your employee requiring a member of the public to repeat a SSN out loud where it can be overheard? The public display, use, and exchange of SSN (including on membership cards carried in wallets) needs to be reconsidered. You place people at much higher risk when you do so.

Understanding identity theft is an important aspect of securing your network and it certainly can help you secure your own personal identity as well.

(Source: http://www.idtheftcenter.org)

Threat Prevention

Threat prevention starts, in many respects, with the IT security project problem statement. What problem are we trying to solve with this project? In other words, what threats do we perceive that we need to address? What is the company trying to protect through these security

measures? What kinds of threats are likely or possible? Are you most concerned about an attack, a theft, or a breach, and which is most likely to occur? Answering these questions will help you define your problem and your outcome statements and help form a solid foundation for your wireless security project plan. In this section, we're going to outline the current threats to wireless networks. Some of this might overlap with other kinds of threats, but it's included here so that you have a fairly comprehensive list in front of you. Clearly, you'll need to do additional research when you sit down to define your wireless security plan because threats change and morph on a regular basis.

In order to understand how to protect your network, you need to understand what you're protecting against. This segment provides detailed information on threats to wireless networks. It should be used in the planning of your wireless security plan, though be clear that this same information can be used to attack your wireless network. It can be used for a friendly penetration test to find weak spots but it can also be used for an unfriendly penetration event to cause harm to your network or company. Most network tools can be used for both good and evil, so don't shoot the messenger.

War Dialing Prevention

War dialing typically occurs during off-hours to prevent phones ringing all over the office, though computers with modems may be turned off after hours, causing you to miss some devices. You may choose, as part of threat prevention, to notify users that if they hear phones ringing, especially after hours, and they are answered with screeching modem tones, that they should report it to the IT security officer. Also, your threat prevention in this case first should be to identify all live modems and phone lines. A scan of your company's phone bill may show existing dial-up lines that everyone had forgotten about (which the phone company just loves). Second, you can war dial your own company (during off-hours to avoid disruption) to see if you find any open modems. If you do so after hours, you risk the chance that users have turned computers off and that existing modems will not answer. If you suspect rogue modems may be a

problem, you'll need to do your war dialing during working hours. Clearly, an e-mail blast letting people know that you're scanning for modems would be counterproductive since the point of the exercise is to *find* modems. If a user with a rogue modem is given a heads up, there's a strong chance you'll never find the modem without going desk by desk and inspecting computers. You can do an inventory of your corporate ownership of Symantec's pcAnywhere and look for existing versions. You can also check system inventory lists and look at all computers that have modems installed. If the modem is not in use and can be removed (as opposed to those that are embedded in the computer's mother board), it should be removed. If it is embedded in the mother board, it should be disabled, if possible.

Once you've gone through and discovered any modems not in use, you next need to check those that are still in use. First find out if they can be disabled. If they are still needed, ensure they require the use of usernames and strong passwords (you'd be shocked how many dial up connections require no username or password) and use the callback feature, if available. Next, look at what software is being used on those dial-up systems and ensure that the latest patches and updates are applied. If the application is deemed to be inherently insecure, look for a newer, better application that could be used instead or a way to divert this dial-up traffic to another connection method. Finally, look at the system and application configuration to ensure it is configured to be as secure as possible. Eliminate unused accounts, disable default or guest accounts, require strong passwords, and so on.

Direct Access

According to statistics from the third World Wide WarDrive, approximately one of every four access points currently deployed is in a default configuration. The default configuration means that there is no encryption enabled and the Service Set Identifier (SSID) has not been changed from the factory settings. The "direct approach" can be used to gain access to wireless networks in the default configuration. The direct approach, in a nutshell, refers to "requesting" a

connection to the access point. This is an extremely simple process in both Windows and Linux. In order to access a wireless network with a default configuration from a
Windows machine, all that you need is a wireless client manager. The wireless client manager is the configuration software that either ships with the wireless card, or is built into the operating system (as is the case with Windows XP). It scans for wireless networks, finds one, and, depending on configuration settings on the client, connects automatically.

Defeating MAC Address Filtering

One security measure that many wireless network administrators put in place is filtering by MAC address. Enabling MAC address filtering allows only network cards with certain MAC addresses to connect to your network. However, as with any security measure, a determined, knowledgeable attacker usually can find a way around such an obstacle.

Most commercial- and consumer-grade wireless networking equipment sends the MAC address clear text even if Wired Equivalency Protection (WEP) is enabled. This means that if you passively sniff the traffic on a wireless network using a freeware tool such as Ethereal (www.ethereal.com), you can determine one or more MAC addresses that are allowed to connect to the network. If MAC address filtering is the only security measure in place, you just need to change your MAC address to one that is allowed access. This is a relatively easy thing to do in both the Windows and Linux environments. In Windows, it's a matter of editing a registry key manually or using an automated tool. In Linux, it's a matter of changing the MAC address in the interface. This also can be done manually using the *ifconfig* command or using an automated tool.

Finding Cloaked Access Points

Many wireless network administrators "cloak" their access points by putting them in "stealth" mode. This is accomplished by disabling the SSID broadcast. Active scanners, like NetStumbler, do not detect cloaked access points. These access points can be found using passive scanners like Kismet or AirSnort. Keep in mind that while you may have cloaked your

access points, an intruder could have installed an access point on your network and cloaked it. Therefore, you need to use these same tools to find cloaked access points that may be attached to your network. One of the biggest benefits that passive scanners like Kismet have to offer is the ability to detect access points that are not broadcasting their SSID. Discovering cloaked access points with Kismet is accomplished by placing your wireless card in monitor mode. Older versions of Kismet required that Kismet be placed in monitor mode manually using the *kismet_monitor* command. When Kismet discovers a cloaked access point, it will initially list it as having no SSID. As Kismet collects more packets, it will be able to determine the SSID.

AirSnort is a passive wireless scanner developed by the Shmoo Group (http://airsnort.shmoo.com). Like Kismet, AirSnort will automatically activate your card in monitor mode when it is started. Any cloaked access points that AirSnort initially finds will project a blank SSID, but after enough packets are collected, AirSnort is able to determine the SSID of the cloaked network. Unlike Kismet, AirSnort has additional functionality that is also extremely valuable to an attacker. We'll discuss AirSnort in more detail later when we look at how one attacks WEP.

Man-in-the-Middle Attacks

Placing a *rogue AP* (an unauthorized access point placed on a network by an individual) within range of wireless stations is a wireless-specific variation of a *man-in-the-middle attack*. If the attacker knows the SSID the network uses (which, as we have seen, is easily discoverable) and the rogue AP has enough strength, wireless users have no way of knowing that they are connecting to an unauthorized AP.

Using a rogue AP, an attacker can gain valuable information about the wireless network, such as authentication requests, the secret key that is in use, and so on. Often, the attacker will set up a laptop with two wireless adapters, in which the rogue AP uses one card and the other is used to forward requests through a wireless bridge to the legitimate AP. With a sufficiently strong antenna, the rogue AP does not have to be located in close proximity to the legitimate AP. For example, the attacker can run

the rogue AP from a car or van parked some distance away from the building containing the network. However, it is also common to set up hidden rogue APs (under desks, in closets, and so on) close to, and within, the same physical area as the legitimate AP. Due to their virtually undetectable nature, the only defense against rogue APs is vigilance through frequent site surveys (using tools such as AirMagnet, NetStumbler, and AiroPeek) and physical security.

Frequent site surveys also have the advantage of uncovering the unauthorized APs that company staff members might have set up in their own work areas, thereby compromising the entire network and completely undoing the hard work that went into securing the network in the first place. These unauthorized APs usually are set up with no malicious intent but rather were created for the convenience of the user, who might want to be able to connect to the network via his or her laptop in meeting rooms, break rooms, or other areas that do not have wired outlets. Even if your company does not use, or plan to use, a wireless network, you should consider doing regular wireless site surveys to see if someone has violated your company security policy by placing an unauthorized AP on the network, regardless of that person's intent.

Hijacking and Modifying a Wireless Network

Numerous techniques are available for an attacker to *hijack* a wireless network or session. Unlike some attacks, network and security administrators may be unable to distinguish between the hijacker and a legitimate passenger. Many tools are available to the network hijacker. These tools are based on basic implementation issues within almost every network device available today.

As TCP/IP packets go through switches, routers, and APs, each device looks at the destination IP address and compares it with the IP addresses it knows to be local. If the address is not in the table, the device hands the packet off to its default gateway. This table is used to coordinate the IP address with the MAC addresses that are known to be local to the device. In many situations, this list is a dynamic one that is built up from

traffic passing through the device and through Address Resolution Protocol (ARP) notifications from new devices joining the network.

There is no authentication or verification that the request the device received is valid. Thus, a malicious user is able to send messages to routing devices and APs stating that his MAC address is associated with a known IP address. From then on, all traffic that goes through that router destined for the hijacked IP address will be handed off to the hacker's machine. If the attacker spoofs as the default gateway or a specific host on the network, all machines trying to get to the network or the spoofed machine will connect to the attacker's machine instead of their intended target. If the attacker is clever, he will use this information only to identify passwords and other necessary information and route the rest of the traffic to the intended recipients. If he does this, the end users will have no idea that this *man in the middle* has intercepted their communications and compromised their passwords and information.

Another clever attack can be accomplished through the use of rogue APs. If the attacker is able to put together an AP with enough strength, the end users might not be able to tell which AP is the authorized one that they should be using. In fact, most will not even know that another AP is available. Using this technique, the attacker is able to receive authentication requests and information from the end workstation regarding the secret key and where users are attempting to connect.

These rogue APs can also be used to attempt to break into more tightly configured wireless APs. Utilizing tools such as AirSnort and WEPCrack requires a large amount of data to be able to decrypt the secret key. An intruder sitting in a car in front of your house or office is noticeable and thus will generally not have time to finish acquiring enough information to break the key. However, if the attacker installs a tiny, easily hidden machine in an inconspicuous location, this machine could sit there long enough to break the key and possibly act as an external AP into the wireless network it has hacked. Once an attacker has identified a network for attack and spoofed his MAC address to become a valid member of the network, the attacker can gain further information that is not available through simple sniffing. If the network being attacked

is using SSH to access the hosts, just stealing a password might be easier than attempting to break into the host using an available exploit.

By simply ARP-spoofing the connection with the AP, the attacker can appear to be the host from which the attacker wants to steal passwords. The attacker can then cause all wireless users who are attempting to SSH into the host to connect to the rogue machine instead. When these users attempt to sign on with their passwords, the attacker is then able to, first, receive their passwords, and, second, pass on the connection to the real end destination. If the attacker does not perform the second step, it increases the likelihood that the attack will be noticed because users will begin to complain that they are unable to connect to the host.

Attacking Encrypted Networks

One of the most common ways that administrators attempt to protect their wireless networks is with encryption. Unfortunately, the two primary means of protection, Wired Equivalent Protection (WEP) and Wi-Fi Protected Access (WPA), have flaws that allow them to be exploited. This section discusses how to attack networks that are protected by WEP and WPA.

The most commonly used form of encryption protecting wireless networks is WEP. WEP is a flawed implementation of the Rivest Cipher 4 (RC4) encryption standard. Scott Fluhrer of Cisco Systems, Itsik Mantin, and Adi Shamir of the Weizmann Institute detailed the flaws in WEP in their joint paper *Weaknesses of the Key Scheduling Algorithm of RC4* (www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf). In short, WEP utilizes a fixed secret key. Weak initialization vectors sometimes are generated to encrypt WEP packets. When enough weak initialization vectors are captured, the secret key can be cracked. There are a two popular tools available on the Internet that can be used to crack WEP encryption.

1. Windows WEPCrack (Windows)

   WEPCrack (http://wepcrack.sourceforge.net) is a set of Open Source PERL scripts intended to break 802.11 WEP secret keys. It was the first publicly available implementation of the attack

described by Fluhrer, Mantin, and Shamir in their paper. Since a PERL interpreter is not installed by default with Windows Server 2003 (or any version of Windows, for that matter), you will need to install one to run the scripts. One or both of the following freely available solutions will give you what you need: Cygwin (www.cygwin.com) or ActiveState ActivePerl (www.activestate.com/Products/ActivePerl). The more robust option is to install Cygwin. Cygwin is a Linux-like environment for Windows that consists of a DLL (cygwin1.dll) to provide Linux emulation functionality and a seemingly exhaustive collection of tools, which provide the Linux look and feel. The full suite of PERL development tools and libraries are available; however, the PERL interpreter is all that is required to run the WEPCrack scripts. The other option, using a Windows-based PERL interpreter, may be desirable if you have no need for Linux emulation functionality on your workstation or server. ActiveState ActivePerl, available by free download from the ActiveState Web site (www.activestate.com), provides a robust PERL development environment that is native to Windows. WEPCrack was written so that it could be ported to any platform that has a PERL interpreter without needing to modify the code.

2. AirSnort (Linux)

   When enough weak initialization vectors are identified, AirSnort begins attempting to crack the WEP key. There are about 16 million possible initialization vectors generated by wireless networks using WEP. Approximately 9 thousand of these are weak. AirSnort considers these 9 thousand weak initialization vectors as "interesting." According to The Shmoo Group, most WEP keys can be guessed after collecting approximately 2 thousand weak initialization vectors.

   After some weak initialization vectors have been collected, AirSnort will attempt to crack the WEP key. A vast majority (approximately 95 percent) of weak initialization vectors provide

no usable information about the WEP key. One way you can try to decrease the amount of time it takes to crack the key is by increasing the crack breadth in AirSnort. According to the Shmoo group's Frequently Asked Questions site for AirSnort (http://airsnort.shmoo.com/faq.html), this will increase the number of key possibilities examined when AirSnort attempts to crack the WEP key.

The most difficult part of attacking wireless networks deployed with WEP encryption enabled is the amount of time it takes. It usually requires a minimum of 1200 weak initialization vectors to crack the WEP key. It can take days or even weeks to capture this many weak initialization vectors.

Once you have the cracked key, it's a simple matter of adding a preferred network in the wireless networking properties (Windows), entering the SSID and the cracked WEP key. In Linux, edit the *wireless.opts* file to include the cracked key and then restart PCMCIA services.

Wi-Fi Protected Access (WPA) networks were discovered to be less secure than originally thought when Robert Moskowitz of ICSA Labs discovered that WPA is vulnerable to an offline dictionary attack, a brute force attack that tries passwords and/or keys from a precompiled list of values (http://wifinetnews.com/archives/002452.html). WPA utilizes a 256-bit preshared key or a passphrase that can vary in length from eight to 63 bytes. Short passphrase-based keys (less than 20 bytes) are vulnerable to the offline dictionary attack. The preshared key that is used to set up the WPA encryption can be captured during the initial communication between the access point and the client card. Once you have captured the preshared key, you can use that to essentially "guess" the WPA key using the same concepts that are used in any password dictionary attack. In theory, this type of dictionary attack takes less time and effort than attacking WEP. Although there are currently no tools available to automate cracking WPA, it is only a matter of time before they are available. If you're using WPA, you should use a long, complex string that is less vulnerable to a dictionary attack than a short, simple one would be.

Legal Liabilities

We discussed legal liabilities in detail in Chapter 9, and if you skipped that chapter for any reason, be sure to read up on the legal issues surrounding IT security these days. The bottom line is that the laws are changing. Requirements are sometimes unclear or conflicting and lack of attention to detail, and lack of "reasonable care" can be cause for litigation in the event of a serious security breach. Companies that are attacked that fail to recover quickly have a 50 percent chance of failing within three years of the attack. Beyond that, your company and its executive team could face stiff penalties if reasonable care is not taken.

With wireless networking on the rise and the price of wireless components falling, it's easy to see how a company could experience a wireless breach perhaps more easily than an attack via the Internet or some other opening. Therefore, you should be sure that your wireless security plan is thorough *and* an assessment should be conducted even if your company does not officially have a wireless network. You never know if your users (or the bad guys) have installed access points until you scan for them. Saying that your company did not install or sanction a wireless network will be no defense if your network is breached and you find yourself being sued by customers whose personal data was stolen.

Business Intelligence…

Lawmakers Crack Down on Wi-Fi Crime

According to an April 26, 2006 article on internetnews.com, by Tim Scannell, if you're a business owner in New York and you use a wireless LAN to handle sensitive customer data, you had better make sure it's secure. Lawmakers in White Plains, New York (Westchester County, north of Manhattan) passed a law making it illegal for a business not to take necessary precautions to protect its wireless networks from accidental or deliberate abuse. The new law is less restrictive of public Wi-Fi hotspots like those found in coffee shops and hotels. While many members of the

Continued

business community support this legislation, not everyone is a big fan of this approach. It's an issue that needs to be addressed, and according to Andrew Neuman, senior assistant to the county executive, "At the end of the day, not one person has said it's a bad idea.

"IBM's corporate headquarters is located in White Plains, and therefore must also comply with the new law, which goes into effect in October. Executives there have not yet responded to the legislation," Neuman said.

Experts from the technical community have a mixed reaction to the legislation.

"Strong authentication and encryption combined with Wi-Fi security technologies will ultimately be the best remedy for keeping the bad guys off the network while protecting users from connecting to unauthorized devices." Some experts are not convinced that forcing businesses to secure their wireless networks is the best approach. "As much as the local government thinks they're doing the right thing by enforcing some sort of wireless security, is it really within their rights to do so?" said Doug DiNunzio, senior product manager for Bluesocket in Burlington, Mass.

To read the full article, head to http://www.internetnews.com/wireless/article.php/3601886.

Costs

Remember that in every project planning process, at some point you should ask the question, "What if we do nothing?" The reason for asking this question is to avoid solving a problem that doesn't actually need to be solved. In the case of wireless security, you can't just "do nothing" if you have a wireless network, but suppose you don't have a wireless network yet, and you're planning security for your proposed wireless network? Now the question makes a bit more sense—in essence "What if we don't have a wireless network?" Don't start with the assumption you *should* have a wireless network just because everyone else does or because it's the latest, greatest thing. If you haven't developed a strong business case for why you should have a wireless network, you've skipped an important step. Most companies these days can make the case for having a wireless network, if only from the perspective of providing flexibility and

avoiding the need to run more cabling. Make sure you start with a clean baseline and add from there. However, even if your firm decides against deploying a wireless network, you can't assume your employees (or vendors, visitors, or intruders) haven't installed wireless access points that create rogue wireless networks on their own. In this case, you would need to look for wireless networks attached to the corporate network on a regular basis as part of your operational security.

Once you've decided to implement a wireless network, you'll need to include the initial and ongoing costs of securing the wireless network to your cost estimates. If you already have a wireless network installed, you'll have to address the cost of the wireless network security component separately, as we're doing here. Your costs include the cost of securing the network to which wireless access points connect, securing the communication between wireless devices (WEP, WPA) and securing the wireless devices themselves (laptops, PDAs). You should also ask yourself whether the cost of securing all of this is worth either having a wireless network or securing the wireless network. Using the hotel guest wireless network example, there's no reason to implement security because it would be an extremely high-maintenance activity to provide secure access to guests who may stay for only a night or two. However, since the WAP has to connect to the Internet, you will need to plan how to provide this access without risking your own network's security.

In addition to these implementation costs, you need to assess the cost to the organization of a wireless security breach. If the network is compromised, how much will it cost you to repair the damage? What are the costs of remediation, legal defense, and possibly marketing/PR to address a potential breach? Finally, you need to look at the cost/benefit analysis to determine how all the potential costs of a breach compare to the cost of securing the network in the first place. Though the answer often comes out in favor of security solutions, you want to be comfortable with your analysis so you can defend it to your executive team or project sponsor.

Time

Perhaps the biggest cost (other than potential legal bills) is the time lost due to investigating and repairing a security breach that occurs, especially a wireless attack that can be a bit more obscure in some ways. As you're probably painfully aware, a security breach takes time away from other IT projects and IT work but it also causes lost productivity for everyone in the organization. Although you may not be able to specifically quantify the cost of a potential security breach in terms of the time it would take to address such a breach, you can certainly look at it from a macro level. If your company is highly dependent on computers and electronic communications, your time costs will be higher than if your company uses computers but doesn't rely significantly on them. Take a look at the cost of downtime and give it an overall assessment if you can't specifically quantify it.

People

The people risk is the risk that is incurred from people's actions. In a wireless networking situation, your people risk is twofold. First, has anyone inside the organization installed a wireless access point? Whether their intentions are good or bad, the result will be the same—a huge security hole that circumvents all the best network security measures you've put in place. Therefore, while you need to assess the risk in this regard, you also need to implement policies regarding the unauthorized implementation of *any* technology, including wireless devices, and you need to implement a procedure for sweeping your network on a regular basis looking for rogue access points.

Another people risk is the risk of users with wireless devices connecting to the network via unsecured channels. If they are working with sensitive data on a laptop and they connect via an unsecured connection from a hotel or airport lounge, there is some danger their wireless communication could be hijacked. Implementing policies and procedures for secure wireless communication for mobile users is key to assessing your risk in this area.

The outside people risk is that a vendor, supplier, or visitor could install a rogue access point anywhere in your building. Assessing the risk includes reviewing the physical environment of your building and finding places an access point could be installed in an unobtrusive manner. Your risk assessment might include a physical risk review to find spots where a WAP could be installed and creating tasks in your project plan to make those spots more secure and/or more visible.

Finally, you'll need to look at the external risk of people who may come in close enough contact with your physical premises to interfere with wireless network operations. This might include RF jamming, intrusion, spoofing, and more.

Impact Analysis

The impact analysis is an essential element in a security project because, as we've stated numerous times, you have to balance the time and cost of implementing security against the potential impact of a security breach. If your company makes nuts and bolts, stores no real confidential information, and doesn't store personal information such as credit card numbers or medical records on your network, the impact of a security breach is far lower than for a high-profile hospital or major university. No doubt a security breach could potentially cause embarrassment and lost productivity if intruders impacted the confidentiality, integrity, or availability of network resources, but the chance you'd end up in a law suit for failing to protect certain data would probably be low. Therefore, it's important that you perform an impact analysis to understand how an intrusion of your wireless network could impact your company. Your analysis should include (but should not necessarily be limited to):

1. Data loss—confidentiality, integrity and/or availability
2. Productivity loss—direct and indirect (what was *not* getting done when the situation was being repaired)
3. Financial loss—direct and indirect

4. Loss of reputation—customers, vendors, employees, public markets
5. Loss of trust and confidence—customers, vendors, employees, public markets
6. Legal or regulatory implications—what are the legal, financial, and regulatory implications

Business Intelligence…

The Proliferation of Wireless Technologies

A recent article on MIT's Technology Review Web site highlights the new ways Wi-Fi technology is being used. Researchers at Brigham & Women's Hospital in Boston are collaborating with Harvard Medical School and MIT to test what they're calling "Scalable Medical Alert and Response Technology" (SMART) for use in ER waiting rooms. Researchers hope this wireless medical technology using sensors will make waiting in the emergency room a bit less life-threatening. The author of the article says: "Here's a scenario: You find yourself sitting in a local emergency room, or standing in the admitting line of an emergency clinic. But instead of just cooling your heels (and having a cardboard tag tied around your neck, as Gulf Coast clinics did after Katrina), you've been given a fanny pack containing a pocket-sized computer and ultrasound transponder. And wires come out of it, leading to a sensor on your finger and some more on your chest. Now, if something happens—say, you quietly go into a cardiac arrest—the doctors will know and can come running." Let's hope hackers don't find a way into this one.

Head to this URL to read the whole story by Lamont Wood dated May 5, 2006:

http://www.technologyreview.com/read_article.aspx?id=16776&ch=infotech

Wireless Security Project Parameters

We've looked at many aspects of wireless networking, the risks and threats, the tools both you and the hackers can use. Now, let's start planning the wireless security project. We'll begin where all projects should begin, with the problem statement and mission statement.

Your problem statement should reflect the current situation in your company, whether you have a wireless network or not. We've included a couple of sample problem statement to get you started; you'll need to tweak it to reflect your company's situation.

> We currently have a wireless network that is unsecured. We also have business users who travel frequently and utilize wireless connections to check e-mail and log into the network. We do not know our level of exposure and we have no security measures in place.

> We currently do not have a wireless network but we do not know if there are ad hoc wireless networks in existence putting our network assets at risk. We have users with wireless devices including laptops and PDAs and want to ensure they are secure when connecting to our network, whether internally (unauthorized wireless networks) or externally.

Your mission or outcome statement should focus on the other side of the problem statement—where do you want to be when your project is complete? We've included two mission or outcome statements to give you a running start.

> We will have a reasonably secure wireless network that will keep out most intruders. We will implement security measures on all wireless mobile devices and create new operating procedures and user policies to support this higher level of desired security.

> We will continue to operate without an official corporate wireless network but will implement IT operational plans that include scanning for rogue wireless networks on our

corporate network. We will also educate users and provide policy guidelines and best practices to keep our corporate mobile users safe when connecting to our network from external locations.

Requirements

As you recall from standard project management, we need to define the various requirements for this project. They include functional (often user-driven), technical, and legal or compliance requirements. It's usually best to start with functional requirements and develop technical requirements from there. We'll discuss functional and technical requirements but as with everything in these project plans, you'll need to tailor it to your specific organizational needs. Remember that, in general, the functional requirements describe "what" and the technical requirements describe "how."

Since wireless network security does not exist in a vacuum, it's important to remember that the solutions you develop for your wireless security project will very likely impact some other project. For example, if you decide you want to implement authentication or encryption protocols, these may impact all remote connections, all wireless connections, all users, and so on. Therefore, be sure to check with other IT security project teams or with your IT security program manager (if one exists) to coordinate the implementation of these across the enterprise. These may end up rolling up into the corporate IT project plan so that all the individual security area project (ISAP) plans coordinate their use of authentication or security protocols. You don't need four different groups identifying and implementing security protocols and work at cross-purposes in the organization.

Some people also like to include "success factors" in project requirements because they want to define what is required to be successful. That is certainly one way it can be documented and if that is the method you use, that's fine. In this methodology, we use "assumptions" (defined later in this chapter) to capture the things we're assuming will be in place so

the project will be successful. There are probably 9 million opinions on how to approach this and the important point is that you do address it either as requirements for success or assumptions about what will be in place to help the project be a success. We've addressed it in the project assumptions.

One very important note here: we have not specifically talked about forming your project team (we'll discuss that later in this chapter), but you would be remiss to formulate your requirements without additional input from your IT staff as well as from key stakeholders. Users, departmental managers, trainers, and HR representatives should be included in defining functional requirements. Your IT team can then translate them into technical requirements. In addition, you will need these same experts to help you define appropriate policies, procedures, and processes for implementing and maintaining wireless security once project work is complete. Building this important information and feedback into your project plan will help you deliver a project that meets diverse organizational needs.

Functional Requirements

Different people phrase functional requirements differently. How you word them is not nearly as important as that you word them to include what you want your wireless project to include by way of functionality. Therefore, the functional requirements for a wireless security project could include:

1. Address physical security—Monitoring and/or restricting access to company's physical premises and network components.
2. Address network components—Identifying and locating all existing authorized and rogue access points and ad hoc networks. Identifying all existing wireless devices and connection methods. Identifying procedures for locating rogues and how they will be addressed.
3. Develop ability to monitor and detect intrusion via wireless access.

4. Develop ability to monitor and manage wireless data confidentiality, integrity, and access.
5. Develop list of network resources to which users should have access (with the understanding that not all resources need to be accessible via remote or wireless connections).
6. Develop policies and procedures to dictate appropriate/secure use and to educate users about maintaining wireless security.

Technical Requirements

Technical requirements for a wireless security project could include:

1. Physical security—Security guards monitoring/controlling building entry/exit (ensuring proper identification, preventing "tailgating" (when one visitor enters right behind another authorized visitor), requiring visitors to sign in or be escorted, etc.), card key access, locked server rooms, locked doors, cabinets, and drawers in public or easy-to-access locations.
2. Address wireless network components—Based on the data provided earlier in this chapter (Threat Assessment), identify the tools needed to locate wireless components on your network.
3. Identify the technical requirements for an intrusion detection/intrusion prevention (IDS/IPS) system that has the ability to monitor and detect intrusion via wireless access.
4. Identify the technical requirements for encryption, secure connections, and secure access via wireless technologies and via Internet connections accessed through wireless connections in a variety of locations.
5. Identify the technical requirements for securing a variety of wireless devices and policies for the use of such devices.
6. Identify the specific technical requirements for users regarding the use of wireless networks and wireless devices on company

premises and off company premises when connecting to the company network and noncompany networks.

7. Identify the ongoing operational procedures related to maintaining wireless security including frequency and method of scanning, physical inspection practices, and maintaining security on user's wireless devices.

You may have other requirements and your technical specifications should be much more specific. For instance, you should identify which assets (laptops, PDAs) you'll use for identifying all existing authorized and unauthorized access points and ad hoc networks. What operating system are these devices using? Which programs will you use for this activity, which version, where will you get it, what else is needed (other equipment, other programs) to perform this activity and what are the specifications of the program (i.e., what does this program need to do?). In some cases, you may be listing the requirements that are used to evaluate and purchase (or download in the case of freeware) a program. In other cases, you may be listing the technical requirements for the laptop, all software applications, antenna, and so on. This is just one example of the specificity you should strive for in your technical requirements. The seven items in the list are representative of the types of technical requirements, but you will probably have a longer list of technical requirements and your list should be far more specific. Here's an example of the level of specificity for a single elements of the technical specifications that would be desirable:

- Dell Inspiron 3500 laptop with 512KB RAM, 40GB hard disk running Windows XP Professional (Asset tag # 44932)
- Orinoco Classic Gold wireless card
- NetStumbler ver. 0.4.0

In addition, you might also specify a number of other tools you want to use in your wireless security project including (but certainly not limited to):

- NetStumbler, MiniStumbler
- Kismet
- WinSniffer
- ettercap
- L0phtCrack
- LRC
- Share Enumerator Legion 2.1
- Network Management and Control—Hyena, LANBrowser, Solarwinds, SNMPc
- Wireless Protocol Analyzers—Wildpackets Airopeek, AirMagnet, Fluke WaveRunner Wireless Tester, Ethereal, and more
- Operating System Fingerprinting and Port Scanning—LANGuard Network Security Scanner
- Networking Utilities – WS_Ping Propack, NetScan Tools Professional

Technical requirements might also include specific training initiatives to ensure staff is trained on key technologies, assessment methodologies, or wireless network detection and intrusion tools. Since hackers are well trained in these technologies, you should ensure your own staff is also well versed in using these tools so that you can at least level the playing field.

Legal/Compliance Requirements

This is an area where you're going to have to do some serious research, talk with your legal, financial, and HR departments and determine exactly which requirements your company must comply with. As we discussed in Chapter 9, there are a wide variety of laws and regulations, and chances are good if you're the head of your IT department that you're already aware of the particular regulations you need to address. However, it's not a bad idea to do some additional research to be sure you've got your bases covered.

Once you're clear which rules, regulations, and laws apply to your business, you'll need to develop a specific list of requirements. In many cases, these can and should be incorporated into your functional and technical requirements. You may choose to keep track of your compliance requirements within your functional and technical specification by flagging them in some manner such as using COMP: at the beginning of a requirements description or by putting them in one section. Since many of the compliance requirements may overlap regular requirements, you'll need to determine the best method for listing compliance-related requirements. For example, some requirements might be both your own requirements and those needed for compliance. Others might be to satisfy compliance issues only. Do you need to know which is which? Maybe yes, maybe no, you'll have to decide. Regardless of your approach, you should be sure to clearly indicate which items are required for compliance and what those compliance requirements are specifically. This should later be incorporated into task details. For example, suppose in order to be compliant with some particular requirement you must use encryption. The compliance requirement doesn't specify which type of encryption or how it is to be implemented. Therefore, you choose to implement WEP. You'll need to include this in your functional (encryption), technical (128-bit WEP), and compliance (data encryption methods) requirements. You'll need to add one or more tasks to your Work Breakdown Structure (WBS) that implement WEP on your wireless network. You'll need to add testing tasks to ensure that the WEP implementation works as specified and that users can connect wirelessly to the network once WEP is implemented. Then, you'll need tasks in your WBS that also document the implementation of WEP as a compliance requirement and generate whatever documentation is required in order to prove compliance.

Policy Requirements

Policy requirements may fall under functional requirements but there's no rule that you can't create your own category of requirements if it helps ensure you cover all the bases. We'll look at policies in more detail in a

later chapter, but for now, we will walk through a few ideas for policies related to wireless security.

User policies—Installation of wireless access points on the company network; use of wireless devices on company premises; use of wireless devices when traveling; appropriate use of unsecured wireless networks when traveling; guidelines for securing confidential data when traveling.

IT policies—Installation of wireless access points on the company network; management and authorization of wireless devices for use on company premises; management and authorization of wireless devices for users who travel; configuration management for company-issued wireless devices; configuration management for noncompany issued wireless devices; procedures for monitoring the presence of wireless networks connected to the corporate network; procedures for monitoring intrusion via the wireless network; emergency response to wireless intrusion event; remediation for response to wireless intrusion event.

Scope

The scope of your wireless security project is based on a number of factors unique to your organization. Your scope statement should identify what *is* and what *is not* part of the project. By defining what is not included, you can be sure that everyone is pretty clear about where this project is headed. Where possible, identify scope using specific, measurable terms. For instance, your scope might include the building located at 123 Main Street but not the manufacturing facility located at 999 South Street since the manufacturing facility does not have a computer network but only standalone manufacturing computers. You might say your scope includes all network segments, all wireless devices including (list all authorized devices). You might say your project includes all devices that run 802.11 or 802.1X but will not address wireless keyboard, mice, overhead projection systems, remote controls for televisions, sound systems or

projectors, nor will it address Bluetooth or RFID. Once you get into the swing of things, you should be able to clearly say what is and is not included and this will give you a great idea of how big this project is (and is not).

Schedule

You may not be able to create any sort of meaningful schedule at this point, but that's fine. What you should do at this point is see if there are any external drivers for your schedule such as hard deadlines, legal or compliance deadlines that must be met, funding events, public market events, and so on. Look around to see if there is anything that would require your project be completed by a specified time. If not, you may have a bit more flexibility on your wireless project schedule than you initially thought. You might also be able to develop a high-level understanding of how long this project is likely to take. How long will it take you to inventory all company-issued wireless devices? It probably depends on whether you have a database of devices with asset tags and device owners or not. If you have to walk around to every user and ask what devices they have, what operating system they're running, what type of wireless connection they use, you're going to need more time. This kind of information can be used to generate a first-pass schedule estimate that tells you this project is three months or twelve months long. If you still can't make a first-pass guess, that's fine but be sure to ask yourself (and your team), "What other information would we need to generate a fairly good ballpark estimate?" That way, you can focus on clarifying that data rather than randomly gathering data that gets you no closer to the answer.

After you create your Work Breakdown Structure, you should be able to create a very tight schedule. Once you finalize the WBS, it will be the schedule you have to commit to and manage against. At this juncture, you'll just need a rough idea of timelines, but be careful here. Any estimate you casually toss around now might come back to haunt you later. People have a strange way of remembering the one thing you wish they'd forget and if you say, "I don't know, I think it should just take a couple of

months," you'll find that 59 days later someone is asking you for the results of your project. What they didn't hear (or didn't want to hear) is that "it *might* take 60 days and that's once we begin working on project tasks." Be cautious about tossing around estimates and if you're really pressed to give an initial estimate, pack it with as many disclaimers as you can. Later, you will have to (and should) commit to a project schedule but at this juncture, it's not much more than guesswork.

Budget

Just as your schedule may be fuzzy at this juncture, the budget may also be vague at the moment. As with schedule, you need to determine if there are any budgetary constraints specifically tied to your wireless security project budget. It's possible there was recently a new allocation for wireless technology in your firm and you can pull from that budget. It's possible there was recently a budget cut and all budgets were slashed 10 percent, which will trickle down into your IT department. Your choice at that point will likely be to slash all your projects by 10 percent or look at your project list and determine which project(s) should take the hit. In fact, this might be the opportunity you needed to kill a dead project that needed to go away but no one had the nerve to cancel it and reallocate those funds to your wireless security project.

Every company will differ in the way it allocates funds for projects and the way budgets are developed. However, your starting point needs to be your requirements list and your scope because those will dictate how big the project is. Once you understand how large the project is, you can begin to balance schedule, budget, and quality to find the optimal mix for your wireless security project.

As with schedule, once you've developed your WBS and your detailed task list, you should have a very clear sense of how much the project will cost and you should be prepared to defend your budget and manage it. The same perils exist as well. If you toss out a number, you can be sure that will be your top number and it's only going down from there, so avoid giving any financial estimates until you have a better idea of what

number is realistic. Many organizations seem to be more tolerant of not knowing an exact budget more so than not knowing an exact schedule. Most companies ask "how long will it take?" before they ask "how much will it cost?" though every company culture is different. If you're pressed for a budget estimate before you have any idea of what it will cost, just say you're working up an estimate and should have one ready by (whenever) but it's too early to provide any estimates. They might not like that answer but it's safer than being held to a randomly generated guess.

Quality

You may have a distinct approach to quality in your wireless security project in mind but if not, you can begin by defining what level of confidence you want in your wireless security. For instance, 100 percent confidence that your wireless network is secure will be costly and time-consuming (not to mention impossible to achieve) and the risks to your network do not support such an iron-clad approach. What if you were 80 percent sure your wireless network was secure, would that be sufficient? It may seem odd to accept less than 100 percent confidence or 100 percent quality but that's not realistic given the time/cost factors involved with that level of quality. Do you want to use military standards for your firm? That's probably over-engineering the solution to a great extent for most companies, so you may choose to implement 80 percent of the DoD standards. You can see that as you begin to look at your approach, you can begin to define quality in meaningful ways.

Keep in mind that the functional and technical requirements also help define quality by the inclusion or exclusion of various requirements. In fact, your technical requirements generally define your initial level of quality and can be used as a great starting place for understanding project quality.

Quality is also supported and developed through proper training. If your team members don't know how to use AirSnort or NetStumbler, there's a good chance that project results will be less than optimal. Identify training needs once you've identified key skills needed (see next

section) and be sure that you have the skills and expertise needed to deliver a quality job.

Finally, understand that quality is as much a mindset as a measurement. Keep your team focused on doing their jobs with 100 percent accuracy. If every task is completed as specified, you should have a high-quality result on the other end of your project work. Therefore, quality can be built in to task details (completion criteria are excellent for driving quality in a project) and quality can be built one task at a time. Focus your team on delivering quality and use the tools at your disposal to monitor and measure quality as you move through your project work.

Business Intelligence…

Quality in Technical Projects

Most people don't like to admit there's something they don't know and technical people are probably at the top of that list. Given that very human trait, it's important that you, as the IT security project manager, create an environment where teammates are encouraged to ask questions, to say "I don't know," and to ask for assistance. Security and project quality are both dramatically reduced when someone is stumbling around trying to figure out an answer without asking for help to avoid looking dumb. When time is of the essence, having someone fiddle around with settings or reading the software's documentation or Help file may not be the most productive use of time, especially if there is someone on the team (or externally) that has the answer and could help. Discovery is a wonderful way to learn, but it's not always the most productive use of time when *time* is of the essence. Having a more experienced team member provide answers, assistance, or even impromptu training is more efficient in some instances, and it can happen only when team members feel comfortable saying "I don't know" or "I need some assistance." Pairing subject matter experts with novices can foster a learning environment. Creating an atmosphere of open teamwork will improve the quality of your project and increase everyone's skills along the way.

Once you have defined your initial scope, schedule, budget, and quality, you also need to look at the relative priority of those parameters. What is your least flexible parameter? Which one absolutely must be met? Which parameter is your most flexible, the one that can "give" if things start going wrong? This is critically important to understand before you launch the project so if you're not clear about your least flexible and most flexible parameters, you need to find out now. Some people misunderstand the nature of this discussion and think it's just a way to avoid responsibility for results. Although some might use it that way, it's important to understand that things will change during the course of the project. As the project manager, you need to understand how to prioritize things and how to make the best decisions for the project. Understanding the least and most flexible parameters will provide you the tools you need to make sound decisions without letting you off the hook for delivering results. If you haven't talked with your project sponsor yet or if you haven't clarified the priorities yet, develop your own assessment of priorities based on your current understanding of constraints and then discuss them with your project sponsor. If there's any disagreement or confusion, be sure to follow up with an e-mail clarifying or reiterating the result of the meeting so there's no confusion down the road.

Key Skills Needed

Throughout this book, we've discussed defining the skills needed before you identify the people for your project because you can keep a more open mind about what you need without filtering it through the people issues you might encounter. For your wireless security project, you'll need a variety of skills and we've provided a list to start you off. Keep in mind it may not include everything you need for your wireless security project or it might include things that you don't need; you will have to fine tune this to ensure it meets the unique requirements of your project.

- Configuring wireless components—MAC address filtering, WEP/WPA, RF cell sizing, active and passive scanners
- Integrating wireless access with network access

- Operating systems—Windows Server, Windows XP, Linux, Macintosh, PocketPC, Windows CE
- Monitoring and sweeping for wireless access points, use of discovery protocol
- Intrusion detection configuration and monitoring
- Wireless tools—NetStumbler, MiniStumbler, Kismet, AirSnort, AiroPeek, FakeAP, PERL, VBScript
- Authentication, encryption—RC4, RC5, DES/3DES, AES (FIPS 197)
- Segmentation, DMZs, VLANs—Firewalls, enterprise wireless gateways, enterprise encryption gateways, routers, Layer 3 switch (switch router), VPN, VPN concentrator, SSH2 Server, RADIUS
- Network layer protocols
  - Layer 2 (Data Link layer)—WEP (all variations such as TKIP), 802.1x/EAP (all variations), Enterprise Encryption Gateways, Layer 2 Tunneling Protocol (L2TP)
  - Layer 3 (Network layer)—Point-to-Point Tunneling protocol (PPTP), IP Security (IPSec)
  - Layer 7 (Application layer)—Secure Shell (SSH), Secure Shell Version 2 (SSH2), Novell Directory Services (NDS or eDirectory), Microsoft Active Directory (AD)
- Client configuration and security
- IP Services
- Staging, testing, and equipment installation
- Documentation—Technical (configuration, specifications), operational, and policy documentation

Key Personnel Needed

The list of needed skills is pretty extensive, so your first task, once you've completed the skills needs assessment, is to match those skills to your current team. Identify any gaps and decide whether you need to fill those gaps with training, hiring, or contracting. One way to discern this is by developing a sort of "gap hierarchy" where the gaps are prioritized based on how big or critical they are. For example, if someone on your team is well-versed in operating systems but isn't up to speed on PDA operating systems, then training might be in order. On the other hand, if you have no one on your team well-versed in secure remote communication methods, including authentication and encryption protocols, you may want to contract out for that skill. However, if you determine that you will have an on-going need for that skill set, you may want to get permission to hire another IT person to complement your team's skills or send one of your existing people to extensive training. You'll have to balance your immediate needs against your long-term needs to find the right mix.

When you get into project scheduling, you'll find out where you have resource constraints including double-booking someone for project work based on a particularly unique skill set they may have. This may lead you to train additional IT staff or to hire an outside contractor to fill in those gaps or help you work around those constraints.

This is also a good time to make sure you know who your project sponsor is and what his or her schedule looks like during the estimated duration of the project. We're assuming you've already been in contact with your project sponsor because that is typically how projects are initiated, but if you haven't identified or talked with your project sponsor, there's no time like the present to do so.

Project Processes and Procedures

The processes and procedures you'll need for your wireless security project are probably much the same as other project processes and procedures. Some additional items that might make sense would be:

- Method for reporting and addressing rogue wireless access points and ad hoc networks
- Method for inventorying and tracking existing wireless assets.
- Method for reporting existing wireless security environment including:
  - Wireless devices in use
  - Wireless networks implemented
  - Location and type of wireless access points in use
  - Existing authentication and encryption methods implemented
  - Known security risks or gaps in existing system
- Developing security checklists including list of wireless equipment (already listed), client side software and installations settings, configuration data, and so on, periodic inventory checks, periodic physical security checks of wireless equipment

Project Team

After you've identified needed skills and determined the key personnel for your team, you should begin forming your project team. In addition to the technical skills mentioned earlier in this chapter, you'll also need to be sure to include key stakeholders on your project team, especially during the definition stage (scope, requirements, etc.). Be sure to include user representatives during the definition phase and also when you begin testing your wireless security solutions. If you devise a solution that only the most savvy IT folks can implement, you'll have a cacophony of dissatisfied users pounding on your door (literally or figuratively). Also be sure to include subject matter experts including those that can help craft policies and procedures. Include those who really enjoy working with detail who can monitor, manage, and create your project documentation. If you have a compliance officer or someone who is tasked with monitoring and managing compliance issues, be sure he or she is also included on the project

team. Finally, you may need someone from legal or who understands legal issues to help guide you as you define the scope of the project and the functional and/or technical requirements to ensure you've got all your bases covered. One way to be sure you've got the right people on the team is to ask, "What else do I need to know?" and "Who else needs to know about this?" Ask this of yourself, your IT staff, and your initial project team. You can always pare down your project participants but if you miss a key player you'll have to deal with the ramifications, which can include missing a key element for the project or just having to deal with the political fall-out of overlooking someone "important."

Identify project team roles so everyone knows how they fit in and what they should be doing. For complex or lengthy tasks (to be defined later), you may assign leads to work with subteams. Also create a team roster with contact information and be sure to have team members identify any times they'll be unavailable (upcoming scheduled vacations or leave, lengthy training or seminars scheduled, etc.) so you can quickly determine early in the project cycle whether you'll need to bring in more people or find ways to fill gaps.

Project Organization

Everyone has a slightly different way of organizing a project, and we discussed a number of general project organizational ideas earlier in the book, so we won't repeat that here. However you choose to organize your project should include the basics such as defining the project team structure, how things will proceed, when meetings will occur, who has to attend, how project status will be reported, how and where documentation should be stored, and so on. For a security project of this nature, you may want to divide your project team into different groups and have different groups test each other's security solutions in a friendly competition. This might help avoid collusion between team members (leaving back doors open) and it might also help ensure that testing is thorough and comprehensive. As we've mentioned a number of times, there's a danger that testing will test the plan and not test the actual security, so

using creative methods to ensure your testing is as thorough as your attackers is an important part of organizing your project.

It is in this phase you should define what type of reporting will be required. One type of reporting for wireless network security that is needed is a list (and map, if possible) of all known, existing wireless access points in the building. This will be updated after the scan takes place once all currently unknown WAPs are also mapped. You'll need to create checklists for network and user wireless device inventories and you'll need to define standard operating procedures for your wireless security project. How are issues tracked and resolved? How are issues escalated? How are reports formatted and to whom are they submitted? All the run-of-the-mill project processes should be defined and modified to meet your project team's needs before proceeding into project work.

Project Work Breakdown Structure

1. Perform wireless network organizational risk assessment
   - 1.1 Develop list of assets requiring protection
   - 1.2 Develop list of network assets requiring protection
   - 1.3 Perform impact analysis
     - 1.3.1 Cost
     - 1.3.2 Time
     - 1.3.3 People
     - 1.3.4 Legal liability
     - 1.3.5 Regulatory issues
   - 1.4 Perform scan for rogue access points or ad hoc networks
2. Perform wireless network vulnerability assessment
   - 2.1 War dialing
   - 2.2 NetStumbling
   - 2.3 Direct access

- 2.4 MAC address spoofing
- 2.5 Cloaked access points
- 2.6 Man-in-the-middle attacks
- 2.7 Wireless network hijacking
- 2.8 Encrypted network attack
- 2.9 RF jamming

3. Define strategy for strengthening wireless security
   - 3.1 Identify all modem connections and define "modem strategy" (keep or transfer to another connection type)
   - 3.2 Limit network resource access via wireless connections
   - 3.3 Define authentication methods to be used
   - 3.4 Define data security or encryption methods to be used
   - 3.5 Define changes to policy needed to strengthen security
     - 3.5.1 IT security policies
     - 3.5.2 IT operational policies
     - 3.5.3 User policies
4. Implement strategy for strengthening wireless security
   - 4.1 Implement strong security on needed modem connections
   - 4.2 Implement security on all wireless network components
     - 4.2.1 Implement MAC address filtering
     - 4.2.2 Suppress SSID broadcasting
     - 4.2.3 Implement WEP or WPA
     - 4.2.4 Implement RADIUS (or equivalent)
     - 4.2.5 Encrypt email
     - 4.2.6 Use HTTPS, SSH where applicable
     - 4.2.7 Use secure FTP (SSH2, SSL) where applicable

- 4.3 Implement security on all wireless user devices
  - 4.3.1 Ensure all user devices operating systems are up-to-date and have all patches installed
  - 4.3.2 Ensure all user devices applications are up-to-date and have all patches installed
  - 4.3.3 Ensure all user devices anti-virus, anti-spyware programs are up-to-date
  - 4.3.4 Ensure all software configurations are secure and correct
- 4.4 Implement security policies

5. Test security implementation
   - 5.1 Test modem security
   - 5.2 Test wireless network security
   - 5.3 Test wireless user device security
   - 5.4 Test various user security configurations
6. Develop security policies and procedures to support security implementation
   - 6.1 Develop policy regarding scanning for rogue AP and ad hoc networks
   - 6.2 Develop policy and procedure for maintaining wireless security
     - 6.2.1 Develop policies and procedures for maintaining physical perimeter security
     - 6.2.2 Develop policies and procedures for maintaining wireless component security (APs, etc.)
     - 6.2.3 Develop policies and procedures for maintaining wireless device security (laptops, PDAs)
     - 6.2.4 Develop policies and procedures for maintaining user awareness and security skills

6.3. Develop policy and procedure for securing and tracking corporate wireless network components (APs, etc.)

6.4 Develop policy and procedure for securing and tracking users' wireless devices

6.5 Develop policy regarding network resources accessible via wireless connections

6.6 Develop policy regarding user practices for maintaining security with wireless devices

6.7 Develop change management policies regarding maintaining wireless security after project completion

7. Document all security assessments and security implementations

7.1 Document result of assessment

7.2 Document security implementations

7.3 Document operational requirements for maintaining security

7.4 Document all compliance-related materials

Just a quick reminder that you should include task details, which can include (but are not limited to):

- Task name (verb/noun format is preferred)
- Task number (if used)
- Task owner
- Task contributors (working on the project task)
- Description of task
- Duration
- Deadline/due date
- Cost
- Completion criteria
- Resources required

- Dependencies
- Constraints
- Applicable technical or compliance requirements
- Specific task risks, mitigation and triggers (if applicable)

Obviously, the more detail you can add to your tasks, the better everyone will understand exactly what it will take to complete the tasks and the entire project. Using subject matter experts to help complete task details will yield the most detailed and meaningful task details.

Project Risks

Project risks are those things that can (and likely will) go wrong during the course of the project. They are things that you should look for and assess, then plan to avoid or mitigate. This is a great job for all the "naysayers" on your team. You want them to find all the things that could possibly go wrong and challenge them to find a way to avoid those problems. The risks to a wireless security project are going to be unique to each organization and they fall along the lines of typical project risks. Your budget might be at risk, you might risk losing key team members to layoffs or you might not have the technical skills you think you have.

Although we've run through this drill earlier in the book, we'll quickly recap here for convenience. First, brainstorm every risk you and the team can think of. Next, rank the risks in order of criticality and likelihood of occurrence. Criticality should be defined so everyone uses the same ranking system. It could be 1 = Devastating, 5 = Mildly annoying, whatever works for your team. Likelihood should be a similar ranking system where 1 = Extremely likely, 5 = Extremely unlikely (in both ranking systems, there would be similarly defined 2, 3, and 4). Rank each risk according to both scales and then take a look at them. Use a bit of human reasoning and see if the final, ranked list actually reflects reality; if not, adjust the ranking manually to reflect what you all believe is realistic and likely. Next, select a cut-off point and agree to address only the top five or top ten risks. You could spend forever dealing with risks and miti-

gation strategies but if one of your risks is "The world might come to an end" there's really not much point in planning for that type of risk and you might as well move on.

For each risk identified, devise a strategy to avoid or reduce the risk. In essence, identify your "Plan B" before you need it. Be sure to look at the *risk* of the avoidance or mitigation strategy as well. Again, you could spend all day looking at risks but if you fail to look at the risk of the mitigation strategy, you could easily introduce far worse risk into the mix.

Once you're confident in your risk and mitigation strategies, develop triggers for each risk. In some cases, you may want to develop several triggers for a particular risk. For instance, if one of your risks is that there is a layoff coming and you don't know if your staff will be hit, you might add one trigger for "announcement of departmental layoffs" so that when this is announced, you begin looking at your Plan B option. A second trigger might be when the actual personnel are identified. You might then implement phase 2 of your Plan B option. Finally, when those personnel have left the building, you might implement phase 3 of your Plan B option.

For some risks, you may want to add milestones to your project plan so you can keep an eye out for them. For example, if one of the risks is that the new equipment you order might not be available at the time you need it (perhaps you're implementing a new technology that is just coming to market), you not only have to create Plan B but you also have to know to implement Plan B about two weeks before the equipment should be ordered. Adding milestones for risks helps keep them in the front of your mind so they don't sneak up on you.

Project Constraints and Assumptions

In a wireless security project, your constraints will be similar to other kinds of projects. They are often time, budget, or talent constraints. Although they should be addressed via your project planning activities, they may not be. For example, you may be constrained by pending litigation, by a pending merger or reorganization, or by a pending layoff. Typically, project constraints are external to your project and generally are

tied to your macro-environment. List these and determine if any of them constitute a "project killer." If so, you need to circle back with your project sponsor and get clarification as to how to proceed. There's no point in firing up a project that is so constrained from the outset that it has little chance of success.

Assumptions can be thought of as the success factors if you're *assuming* certain conditions will be available during the course of the project. If you delineated success factors in your requirements, you may choose to list them as assumptions here as well. The reason for defining your assumptions is twofold: first, you want to make sure that you're looking at the project with eyes wide open; second, you want to document the assumptions you're making because if any of those things change, it probably will change the outcome of the project. For instance, if you assume that you will be able to schedule time to perform penetration testing and your Vice President of Information Technology comes back to you and says under no circumstances will you perform penetration testing, that may be a major setback to your project plan. If this is listed as an assumption, you can gain agreement from your project sponsor about these assumptions. Then, if things change later, you'll at least have documentation showing that it was listed as an assumption (or success factor), that it was approved by the project sponsor, and that it later changed and had a negative impact on the project outcome.

Project Schedule and Budget

You've created your detailed Work Breakdown Structure and you've developed your task details. At this point, you should be very clear about your project's projected schedule and budget.

The schedule should be defined by placing your tasks in optimal order, then by identifying dependencies. Constraints and conflicts should then be addressed to generate you first real project schedule. Since we're assuming you're familiar with basic project management principles, we won't go into project scheduling techniques. Of course, using a project management software program greatly assists in creating and managing a

project schedule, so now would be the time to input project tasks and generate your schedule if you're using a software program. Software programs are also very helpful at identifying the critical path so you can properly manage those key elements.

As for your schedule, once you've delineated all your tasks, you should also be able to generate a real budget based on the cost of project tasks, the cost of labor (if you track labor costs with your projects), and the cost of training and other auxiliary elements.

A quick reminder about both schedule and budget—don't pad them. Make your schedule and budget estimates as tight and accurate as possible, then add a "management reserve" that provides a general buffer against unexpected changes to your schedule or budget. In this way, you'll be able to see more clearly what you planned on doing and what you were actually able to do. If you pad your estimates, you'll never really know what you thought you could accomplish vs. the padded estimate.

Wireless Security Project Outline

1. Perform wireless network organizational risk assessment.
2. Perform wireless network vulnerability assessment.
3. Define strategy for strengthening wireless security.
4. Implement strategy for strengthening wireless security.
5. Test security implementation.
6. Develop security policies and procedures to support security implementation.
7. Document all security assessments and security implementations.

Summary

We've covered a lot of territory in this chapter. We looked at wireless security from end to end starting with auditing wireless security. There are numerous kinds of wireless devices, not all of which you'll need to address in your wireless security plan, but if you are unaware of these device types, you won't know if they pose a threat or not. We also looked at the basics of wireless technology reviewing the 802.11 IEEE standard.

Understanding the threats in the wireless world requires a deep understanding of how attackers work and the tools they use. We reviewed some of the threat types including war dialing, wardriving (NetStumbling or stumbling), and Bluetooth attacks. In order to develop a useful wireless security project plan, you'll need to perform a risk assessment for your organization. By dividing this assessment into people, process, and technology and by looking at confidentiality, integrity, and availability of data, you can develop a holistic view of your company's risk profile. Since you'll always have to balance security, cost, and practicality, you'll need to assess and evaluate your company's risk profile and risk tolerance to determine how much security is needed, reasonable, and feasible.

Understanding what assets you're actually protecting helps you develop a sound wireless security plan. Assets such as customer credit cards, health care information, financial or bank data, employee lists, trade secrets, intellectual property, and R&D data are high on the list of valuable data assets to be protected. In addition, there are network assets that should be protected including usernames, passwords, directory listings, network firewalls, routers, switches, IP addresses, and ports/protocols in use. This is information that intruders often use to gain access to the valuable data assets or to simply create havoc on the network. An impact analysis helps you understand the ramifications of a potential wireless network intrusion. These elements include data loss (confidentiality, integrity, availability), productivity loss, financial loss, as well as the less tangible but very real problems of losing your company's good reputation or losing the trust and confidence of your customers. There are also legal or regulatory implications that must be assessed.

After going through this material, we began walking through the steps needed to create a meaningful wireless security project plan. We identified the problem, the mission or desired outcome, and the solution. The project definition includes identifying the functional requirements that lead, in most cases, to the technical requirements. We also identified other types of requirements that could potentially apply to your wireless security project including legal or compliance requirements and policy requirements. There certainly are some areas of overlap between the wireless project and other IT security projects, including authentication and encryption, that should be tied in to other projects as applicable.

Developing the project scope, initial estimated schedule, budget, and quality were reviewed with an eye toward the unique elements found in a wireless security project. We were then able to define the skills needed for this project. Though your list of skills will differ from the list provided, it got you thinking in the right direction in terms of the specific skills needed for a wireless security project, which differ in some ways from other IT projects. Once your skill set is defined, you're ready to identify the people needed for the project and to begin forming your project team.

With a project team in place, your next major task together is to create the Work Breakdown Structure. It includes all the major and minor tasks needed to secure your wireless network including the assessment, design, and implementation of a security solution and, of course, the documentation of all security changes made.

The risks, assumptions, and constraints are unique to every company and every IT project, so there's no specific information that can be provided that will fit all organizations. Defining these three key elements is critical to project success, so be sure you walk through these steps and clearly articulate these items.

Finally, we provided a quick outline for you to use in developing your wireless security project plan, as a quick recap for you. Throughout this chapter, we've looked at the standard project management methodology with an eye toward developing a sound wireless security project plan. You should have a solid idea of where to start your own wireless security project plan and, utilizing the information in this chapter, you should be able to take it from here.

Solutions Fast Track

Wireless Security Auditing

- ☑ Intruders and hackers look for the easiest targets first and often will skip over targets that are secured.
- ☑ There are a growing number of wireless devices and wireless protocols in use in the market today, making wireless security an even more important security project.
- ☑ It's important to understand types of threats, including war dialing, wardriving, and Bluetooth attacks.
- ☑ Risk assessment should include the types of assets to be protected. This includes sensitive or confidential data as well as certain network data such as usernames, passwords, or directory structures.
- ☑ Threat prevention runs the gamut from shutting down modems to implementing MAC address filtering, suppressing SSID broadcasts, and implementing various security measures such as authentication and/or encryption.
- ☑ An impact analysis should include the cost in time and money of a potential breach as well as the less tangible costs such as loss of reputation, trust, or confidence. It also should include the legal liability of such an intrusion.

Project Parameters

- ☑ Project parameters begin with defining the project's problem statement, mission, or outcome statement and defining the appropriate solution for the project.
- ☑ Requirements should be defined early in the project definition stage because they essentially define the scope of your project.

- ☑ Requirements include functional, technical, legal, and regulatory (compliance) requirements.
- ☑ Some people include success factors in the requirements since these factors are required for project success. Others include success factors in the assumptions section of the project plan.
- ☑ Scope, schedule, budget, and quality can be defined after the initial project definition is complete and after the requirements have been clearly delineated.
- ☑ Key skills can be defined after the technical requirements are defined and the list should be comprehensive.
- ☑ Key personnel can be matched to the project based on the required skills for the project. If there are any gaps, you can begin planning how to address those gaps including providing training, hiring outside contractors, or creating and hiring a new position.

Project Team

- ☑ You should have identified key stakeholders early in the definition phase in order to help craft the definition so the project would meet many stakeholder needs.
- ☑ The project team will be comprised of a variety of different kinds of team members, some of whom may participate only in some phases of project work.

Project Organization

- ☑ Organizing a wireless security project is fairly standard and should include developing appropriate processes and procedures for your team.
- ☑ Project status reporting, issues logs, error reports, and more should be developed during this phase.

- ☑ Be sure to include processes related to regulatory or compliance activities and documentation in your project plan.

Project Work Breakdown Structure

- ☑ A Work Breakdown Structure for a wireless security project plan was developed outlining the seven major tasks.
- ☑ Subtasks were defined for many of the tasks; your WBS will be different.
- ☑ Task details should be developed with attention to detail. The more clearly defined the tasks are, the more clear the project itself becomes. Quality is built into projects through well-defined tasks.

Project Risks and Mitigation Strategies

- ☑ There are numerous risks to a wireless security project as there are with any IT project.
- ☑ All risks should be identified then ranked. The ranked list should be shortened to the highest overall risks identified.
- ☑ Mitigation strategies, risk analysis of the mitigation strategies, and triggers should be identified for all risks.

Project Constraints and Assumptions

- ☑ Constraints are any elements that may hamper your project's success. These are often found outside of the immediate project environment.
- ☑ Assumptions are those things you are taking to be true or in existence and upon which your project's success rests. Some use assumptions in place of success factors.

Project Schedule and Budget

- ☑ Once you've defined your WBS in detail, you should be able to develop a realistic schedule.
- ☑ If you have project management software available to you, this is a good time to input your tasks and schedule into the program to allow the software to assist you in creating a schedule and identifying the critical path.
- ☑ Budgets can be developed by adding the cost of all tasks plus any administrative costs or costs that apply across the project that cannot (or should not) be attributed to any one particular task.
- ☑ Be sure to include the cost of training, compliance, and any other auxiliary project costs.
- ☑ Avoid padding your estimates. Instead, create accurate estimates then use a "management reserve" to adjust your schedule or budget.

Wireless Security Project Outline

- ☑ An outline was provided to give you the major steps in your project plan.
- ☑ You can modify this outline to suit your needs but it can serve as a good starting point for planning your wireless security project.