

Chapter 2

Risks and Threats of Wireless

This chapter discusses the general goals for information security and how they are used to measure risk and understand threats. This information will help in the next sections of this chapter where each of the threats relating to the many types of wireless communications is explored. After looking at each of the threats, this chapter focuses attention on wireless hackers. In this chapter, we see how hackers locate the existence of wireless networks as well as how law enforcement tracks down these hackers.

2.1 Goals of Information Security

When looking at information security, one must address the three tenets of information security: (1) confidentiality, (2) availability, and (3) integrity. These long-standing goals will help us understand what we are trying to protect and why. This information will help when one starts looking at all the risks and threats that face wireless communications. Before one can properly evaluate risk, one needs to set a baseline to understand the definition of each goal one is trying to uphold.

2.1.1 Confidentiality

Attacks on the confidentiality of information relate to the theft or unauthorized viewing of data. This can happen in many ways, such as the interception of data while in transit or simply the theft of equipment on which the data might reside. The goal of compromising confidentiality is to obtain proprietary information, user credentials, trade secrets, financial or healthcare records, or any other type of sensitive information.

Attacks on the confidentiality of wireless transmissions are created by the simple act of analyzing a signal traveling through the air. All wireless signals traveling through the air are susceptible to analysis. This means there is no way to have total confidentiality because one can still see a signal and subsequently record it. The use of encryption can help reduce this risk to an acceptable level. The use of encryption has its own flaws, as seen later in this book. For the most part, the encryption is secure itself, although how it is implemented and how key management is handled may produce flaws that are easily exploited.

2.1.2 Availability

Availability is allowing legitimate users access to confidential information after they have been properly authenticated. When availability is compromised, the access is denied for legitimate users because of malicious activity such as the denial-of-service (DoS) attack.

Receiving RF signals is not always possible, especially if someone does not want you to. Using a signal jammer to jam an RF signal is a huge problem that has been facing national governments for years. Looking for the availability of RF local area networks (LANs), one notices that performing a DoS attack is easy to accomplish. This is due to the low transmit power allocated by the U.S. Government and poor frame management techniques included in most of the current day wireless standards.

2.1.3 Integrity

Integrity involves the unauthorized modification of information. This could mean modifying information while in transit or while being stored electronically or via some type of media. To protect the integrity of information, one must employ a validation technique. This technique can be in the form of a checksum, an integrity check, or a digital signature.

Wireless networks are intended to function in an unimpaired manner, free from deliberate or inadvertent manipulation of the system. If integrity is not upheld, it would be possible for an attacker to substitute fake data.

This could trick the receiving party into thinking that a confidential exchange of data is taking place when in fact it is the exact opposite. Wireless networks have adapted to this type of threat over time. One can see this advancement as new security standards emerge, creating increasingly complex integrity checks.

2.2 Analysis

Analysis is the viewing, recording, or eavesdropping of a signal that is not intended for the party who is performing the analysis. All RF signals are prone to eavesdropping; this is because the signal travels across the air. This means anyone within the signal's path can hear the signal. One of the only protections available to prevent the loss of confidentiality is encryption. If a signal is using encryption, then its confidentiality can be upheld until that form of encryption is defeated. The risk of analysis on an RF signal is an inherent risk that cannot be avoided. The only option is to mitigate the risk with some type of confidentiality control.

2.3 Spoofing

Spoofing is the act of impersonating an authorized client, device, or user to gain access to a resource that is protected by some form of authentication or authorization. When spoofing occurs in wireless networks, it primarily involves an attacker setting up a fake access point to get a valid client to pass authentication information to that attacker. Another way attackers spoof is by performing a man-in-the-middle attack. In this scenario, an attacker would position himself between a client and the network. This could be accomplished by spoofing a valid access point or by hijacking a session. Once this part is complete, the attacker would then use the authentication information provided by the client and forward it to the network as if it originally came from the attacker.

2.4 Denial-of-Service

Denial-of-service (DoS) is the effect of an attack that renders a network device or entire network unable to communicate. Hackers have found that certain crafted packets will make a network device unresponsive, reboot, or lock up. They have used this technique to shut down high-traffic networks and Web sites. They have also used this attack to reboot network equipment in an attempt to pass traffic through the device as it

is booting up. This is done to try to circumvent any policies set up on the device to protect it or devices behind it. The DoS threat can also adversely affect the availability of a network or network device.

Wireless DoS attacks can be achieved with small signal jammers. Finding signal jammers is not as difficult as one might think. Some modern-day wireless test equipment can perform jamming. This is not the tool's intended purpose, although it is commonly used for this. Jamming is possible because the government regulates the amount of power allowed on a wireless network. In relation to wireless LANs, the amount of power used is a very small amount. This means that it is not difficult to overpower an existing device with a home-made one.

Another DoS threat relating to LANs in particular is the poor structure of management frames. These frames allow for anyone who can analyze the wireless signals to perform a DoS attack by replaying certain management frames. Mostly, these attacks are layer two frame attacks. These attacks try to spoof management traffic, informing the client that he is no longer allowed to stay connected to the network. [Chapter 13](#) discusses these attacks in more detail.

2.5 Malicious Code

Malicious code can infect and corrupt network devices. Malicious code comes in many forms: viruses, worms, and Trojan horses. People often confuse the three main forms of malicious code. Because of this, they use these terms interchangeably. This section looks at each of these and identifies what classifies them into each of the three groups. Viruses infect devices and do not have the ability to replicate or spread outside the infected system on their own. Once a virus infects a machine, it can only replicate inside the infected machine. This means that all threats from viruses stem from receiving infection. The threat of worms is much higher because they can spread across the enterprise and out to the Internet, infecting multiple devices. In the past few years, humans have started to see global worms that propagate across the entire world. The final malicious code threat discussed here is the Trojan horse. This threat comes from installing or running programs that can have or within their use execute code that might contain malicious content.

Malicious code relating to wireless has to do with new viruses that can affect the many new types of wireless end devices such as PDA units, smart phones, PDA phones, laptops, etc. Wireless viruses have just started to appear in the wild. Even with this threat just starting to develop, many forms of wireless malicious code have already appeared. Some of this code has enough intelligence to find and utilize a variety of available wireless technologies on a device to spread even further.

Another form of malicious content relating to wireless is *spam*. Although spam is not destructive in nature, the time and money it costs an organization often makes it seem as malicious. Spam is not just related to wireless. Long before wireless spam there was e-mail spam. Today's wireless devices are capable of receiving messages in many formats: e-mail, text messaging, instant messaging, and voice calls. All of these are starting to see spam pop up on them. Dealing with spam has created a security market of its own with products, solutions, and services created to combat this threat.

2.6 Social Engineering

Social engineering is the often called low-tech hacking. It involves someone using the weakness of humans and corporate policies to obtain access to resources. Social engineering is best defined as tricking or manipulating a person into thinking the party on the phone is allowed access to information, which they are not. The threat of social engineering has been around for quite some time. Some of the most well-known computer hackers used this type of attack to get information. The real threat to this is the skill level involved. No one needs to be computer savvy or a technical genius to perform this type of attack. There are a number of things to do to prevent this type of attack. First, make sure that a policy is in place regarding sensitive information and phone usage. Make sure that not anyone can call and reset someone's password. Create a help-desk identification process to authenticate callers to the help-desk operators.

2.7 Rogue Access Points

Rogue access points pose a major threat to any organization. This is because of the high availability and the limited security features of off-the-shelf access points. If a company does not approach the WLAN (wireless local area network) concept fast enough, frustrated employees will take it upon themselves to start the process. When this happens, employees often put in wireless systems of their own. Even with most current-day access points supporting advanced security standards, the default configuration of an out-of-the-box access point is set to the least secure method. This has created a real threat because now a user can easily bring in a rogue access point, plug it in, and put the entire network at risk. The knowledge level required to install an off-the-shelf access point has almost become plug-and-play today. This means that more and more people have the ability to place rogue access points. These same

people lack the ability to secure these devices or even understand the risk they are posing for the company.

Most access points come from employees, although as we will learn later there are cases where an attacker would try to set one up for easy return access. This was not a big issue until recently when the price of 802.11b access points fell well below \$100. To do this, an attacker would need physical access and a network port. If a hacker wanted access bad enough, spending \$100 for it would be a conceivable expense.

With companies investing in stronger security mechanisms, it would be a shame to have an incident in which an attacker gains access through a non-secure rogue access point. Because of the threats associated with rogue access points many companies have started to put controls in place to increase awareness and prevent the deployment of rogue access points. Many companies that jumped into the newly formed wireless security market have adapted and created tools to detect rogue access points. Some companies have handled rogue access points by creating policies about wireless usage and strict penalties for rogue access placement. Others have taken a second route and invested in wireless intrusion detection systems (WIDS) software.

2.8 Cell Phone Security

Now we will have a discussion of general cell phone identification and security. Cell phones have had a slight advantage over other types of wireless communications in the security realm. This is due to their overwhelming numbers. Most people today have a cell phone; and with so many people using cell phones, many security risks and subsequent controls have been developed to counter each other. Understanding this information will show how cellular phone providers have mitigated similar risks that face wireless local area networks.

Cell phones send radio frequency (RF) transmissions on two distinct channels: (1) one for actual voice communication and (2) the other for control signals. This control signal identifies itself to a cell site by broadcasting its mobile identification number (MIN) and electronic serial number (ESN). When the cell tower receives the MIN and ESN, it determines if the requester is a legitimate user by comparing the two numbers to a cellular provider's subscription database. Once the cellular provider has acknowledged that the MIN and ESN belong to one of its customers, it sends a control signal to permit the subscriber to place calls.

Like all RF devices, cell phones are vulnerable to eavesdropping and spoofing. In the cellular phone industry, these are called "call monitoring" and "cell phone cloning." Another risk associated with cell phones is the

ability to reprogram phones, transforming them into advanced microphones capable of recording and transmitting sound from their location to anywhere in the world.

Monitoring calls is an easy task, especially for phones that use analog technology. This is because most analog cell phone technologies were transmitted in the same band as FM radio. A commonly available radio frequency scanner could get one up and listening to calls in minutes. With the proliferation of digital cellular networks, more and more security was erected. This was great because inside a service provider's network, your calls were, for the most part, safe. There were easier analog targets for criminals to exploit. One's digital phone was not so safe if one roamed or went outside of a provider's area of coverage. When two cellular providers wanted to hand off calls to each other for billing purposes, they converted them to analog so they had a common protocol for interoperability. This also meant that security was no longer present. So, even with a digital phone, once the MIN and ESN are removed or identified from the phone call, it could still be tracked, cloned, or monitored inside the digital network.

Another trick involves turning a cellular telephone into a microphone and transmitter. This can be used to record a conversation or bug a room. This can be done without your knowledge by police, governments, and even some highly educated people. How does it work? It is easy to do, just send a maintenance command on the control channel to the phone. This command places the cellular telephone in a diagnostic mode. When this is done, conversations in the immediate area of the telephone can be monitored over the voice channel. The signal engages the phone to perform this monitoring action without any indication of it taking place. The user does not know the telephone is in the diagnostic mode and transmitting all nearby sounds until he or she tries to place a call. The calling feature does not work and the phone is useless until the power is cycled. After that, the phone returns to a normal state as if nothing ever happened.

This is very scary because the user has no idea he is bugged by his own phone through the airwaves. This threat is the reason why cellular telephones are often prohibited where classified or sensitive discussions are taking place. Someone could be bugging your phone as you read. Do not worry; as long as one can place a call without cycling the power, you're ok.

One publicized case of cell phone monitoring involved former Speaker of the House of Representatives, Newt Gingrich. A call between Gingrich and other Republican leaders was monitored and taped. The conversation concerned Republican strategies for responding to an ethics violation for which Gingrich was being investigated. This call was given, or most likely sold, to the *New York Times* and made public.

Another publicized case of cell phone monitoring involved a pager system instead of a cellular phone system. In 1997, the Breaking News Network monitored the pager messages of a large number of New York City leaders, including police, fire, and court officials. The messages recorded were considered too sensitive to send over the government's protected police radio. This confidential information was captured and then sold to other news agencies in order to get the scoop on a story. This ended up happening sometimes before the police dispatch even had the information. Later in the year, police arrested the officers of this New Jersey news company for illegally monitoring their pager systems.

Next we look at cellular phone cloning. What is cell phone cloning? It is the copying of the unique identification information programmed into your cell phone by a cellular provider. The cellular provider programs the phone with an electronic serial number (ESN) and mobile identification number (MIN). A cloner will steal this information, copy it to a different phone, and place calls on your bill.

There are many ways for cloners to obtain these numbers. One is when someone fixes your phone or even when you buy a new phone at the store, someone could copy this information during the activation process. The MIN and ESN can also be obtained by an ESN reader (see [Figure 2.1](#)), which is similar to a cellular telephone receiver designed to monitor control channels. The ESN reader captures the MIN and ESN as they are being broadcast from a cellular telephone to a cell tower. This happens when your phone is turned on or when you move from one cell phone tower to another.

A major controversy grew around cell phone cloning. At first, the phone companies refused to admit that their security was compromised, thus making the victim pay for all the calls placed by the cloner. This proved to be a big problem for cell phone companies and their customers.

Another threat related to cellular phones deals with the short messaging service (SMS). This is a method of sending short messages similar to e-mail. One of the threats related to this has to do with mass SMS messages that create a denial-of-service attack. This sort of attack has not been widely seen yet, although many industry leaders have openly spoken about the risk and impact if it were to happen.

2.9 Wireless Hacking and Hackers

Inherently, RF has many threats, including interception, signal jamming, and signal spoofing. Because RF travels through the air, picking up the signal is as easy as being within the radio waves' vicinity with the right hardware. Spectrum analyzers can detect radio transmissions showing the

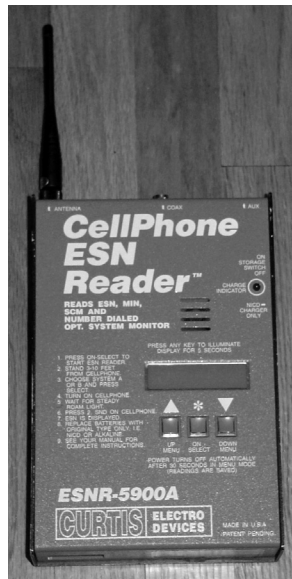


Figure 2.1 ESN Reader.

user the signal frequency. Depending on that frequency, an attacker might be able to identify the transmission right away. Most RF frequencies in the spectrum are reserved for specific uses. Once one is able to find a signal and map it to a reserved spectrum, one knows who is transmitting it and, in some cases, why.

Getting more in tune with the majority of RF threats, one can look at today's RF local area networks (LANs). These, of course, have the same threats as all RF signals, although they do add a new dimension stemming from mass use and scrutiny. Just like cell phones, the more people who use them, the more time people spend looking at how they work and what they can do to defeat any security that exists. This has been seen over the past few years as a large number of users started deploying wireless networks and security flaws began to pop up. Most wireless network setups are capable of working right out of the box. This has led more and more nontechnical people to deploy them. When setting up a wireless LAN right out of the box, the default configurations are usually the most insecure ones.

2.9.1 Motives of Wireless Hackers

America's laws and law enforcement agencies have taught us that rarely is a crime committed without a motive. With this said, if someone was

to spend the time to compromise an RF signal, there always is a motive. Some of these motives can be as harmless as wanting an Internet connection to send a loved one an e-mail, or as terrible as committing an act of terrorism against a nation or government. To understand why someone would try to compromise an RF signal, take a look at some of the more well-known motives, such as to get a free Internet connection, commit fraud, steal sensitive information, perform industrial or foreign espionage, and — the worst of all — terrorism. After understanding what motive or motives an attacker might have, one can better understand how much security one should apply to the RF signal. If a company deals with financial information, it probably is more at risk from an attacker than a small doll shop. Knowing who might attack and why can help ensure that the correct risk-reducing actions are taken.

2.9.2 War Drivers

After more and more people realized that out-of-the-box wireless LANs were generally set up, by default, in the most insecure mode, people started to exploit them. This new fad of identifying and categorizing wireless networks based on their security level has been coined “war driving” (see Figure 2.2). War drivers use equipment and software to identify wireless networks. War driving allows attackers to understand the security associated with any particular wireless network they happen to pass. This equipment not only allows war drivers to identify, locate, and categorize wireless networks, but also allows them to upload their results



Figure 2.2 War drivers.

