291_WarDriving_01.qxd 2/12/04 11:42 AM Page 1

# Chapter 1

# Learning to WarDrive

## Solutions in this Chapter:

- The Origins of WarDriving
- Tools of the Trade or "What Do I Need?"
- Putting It All Together

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 2



# Introduction

Wireless networks have become a way of life in the past two years. As more wireless networks are deployed, the need to secure them increases. This chapter provides background on one effort to educate users of wireless networks about the insecurities associated with wireless networking. This effort is called WarDriving.

This chapter presents a brief history of WarDriving and the terminology necessary to understand what WarDriving is all about. This includes information on why the activity of driving around discovering wireless access points is called WarDriving, some misconceptions associated with the term, and the truth behind the idea of WarDriving. This chapter also discusses the legality of WarDriving.

In order to successfully WarDrive, there are some tools, both hardware and software, that you will need. These tools are presented along with cost estimates and some recommendations. Since there are hundreds of possible configurations that can be used for WarDriving, some of the most popular are presented to help you decide what to buy for your own initial WarDriving setup.

Many of the tools that a WarDriver uses are the same tools that could be used by an attacker to gain unauthorized access to a wireless network. Since this is not the goal of a WarDriver, the methodology that you can use to ethically WarDrive is presented.

WarDriving is a fun hobby that has the potential to make a difference in the overall security posture of wireless networking. By understanding WarDriving, obtaining the proper tools, and then using them ethically, you can have countless hours of fun while making a difference.

# The Origins of WarDriving

WarDriving is an activity that is misunderstood by many people. This applies to both the general public, and to the news media that has reported on WarDriving. Because the name "WarDriving" has an ominous sound to it, many people associate WarDriving with a criminal activity. Before the discussion of how to WarDrive begins, you need to understand the history of WarDriving and the origin of the name. The facts necessary to comprehend the truth about WarDriving, as well as why the media has incorrectly reported on WarDriving are provided.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 3



# What's in a Name?

WarDriving is the act of moving around a specific area and mapping the population of wireless access points for statistical purposes. These statistics are then used to raise awareness of the security problems associated with these types of networks (typically wireless). The commonly accepted definition of WarDriving among those who are actually practitioners is that WarDriving is not exclusive of surveillance and research by automobile – WarDriving is accomplished by anyone moving around a certain area looking for data. This includes: walking, which is often referred to as WarWalking; flying, which is also referred to as WarFlying; bicycling, and so forth. WarDriving does NOT utilize the resources of any wireless access point or network that is discovered without prior authorization of the owner.

## The Terminology History of WarDriving

The term WarDriving comes from WarDialing, a term you may be familiar with being that it was introduced to the general public by Matthew Broderick's character, David Lightman, in the 1983 movie, *WarGames*. WarDialing is the practice of using a modem attached to a computer to dial an entire exchange of telephone numbers (often sequentially—for example, 555-1111, 555-1112, and so forth) to locate any computers with modems attached to them.

Essentially, WarDriving employs the same concept, although it is updated to a more current technology: wireless networks. A WarDriver drives around an area, often after mapping a route out first, to determine all of the wireless access points in that area. Once these access points are discovered, a WarDriver uses a software program or Web site to map the results of his efforts. Based on these results, a statistical analysis is performed. This statistical analysis can be of one drive, one area, or a general overview of all wireless networks.

The concept of driving around discovering wireless networks probably began the day after the first wireless access point was deployed. However, WarDriving became more well-known when the process was automated by Peter Shipley, a computer security consultant in Berkeley, California. During the fall of 2000, Shipley conducted an 18-month survey of wireless networks in Berkeley, California and reported his results at the annual DefCon hacker conference in July of 2001. This presentation, designed to raise awareness of the insecurity of wireless networks that were deployed at that time, laid the groundwork for the "true" WarDriver.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 4



## WarDriving Misconceptions

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. 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.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 5



Notes from the Underground…

## Warchalking Is a Myth

In 2002, the news media latched onto something called warchalking. Warchalking is the act of making chalk marks on buildings or sidewalks to denote the presence and availability of wireless networks. Playing off of the practice of hobos during the Great Depression who would mark homes or areas to communicate information about the area to other hobos, warchalkers use a series of symbols to alert others as to what type of wireless network they will find in that area. Three primary symbols used by warchalkers are illustrated in the following figures. Figure 1.1 indicates an open node, or one in which WEP encryption is not utilized and individuals are encouraged to use. The Service Set Identifier (SSID) or network name is chalked above the symbol and the available bandwidth speed is chalked below the symbol.

**Figure 1.1** The Open Node

**Figure 1.2** The Closed Node

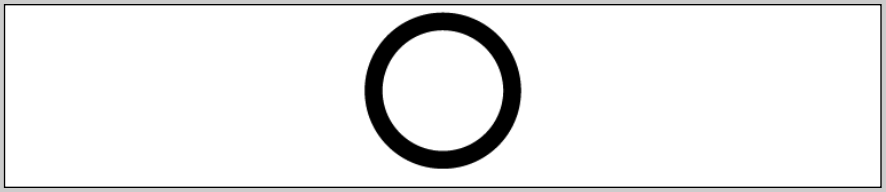


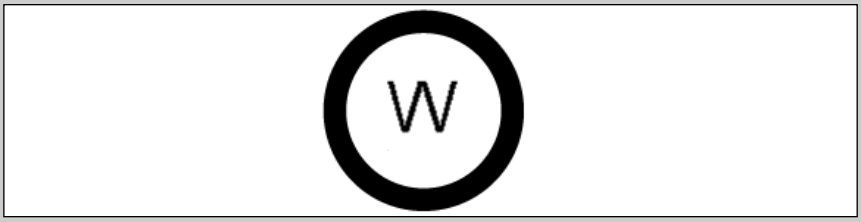
Figure 1.2 indicates a closed node. One that is not open for public use. The SSID or network name is chalked above the symbol and nothing is chalked below the symbol.

Continued

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 6



**Figure 1.3** The WEP Node




The symbol in Figure 1.3 indicates a node with WEP encryption enabled. This should be viewed as an unequivocal stop sign. The SSID and contact information to arrange for authorized access are chalked above the symbol and the available bandwidth is chalked below the symbol. Aside from hot spots such as Starbucks, there have been very few actual sightings of warchalked wireless networks. Despite the media hype surrounding warchalking, it is generally viewed as a silly activity by WarDrivers. A recent poll on the NetStumbler forums (https://forums.netstumbler.com) was unable to find even one person that had actually chalked an access point. The results of the survey can be seen in Figure 1.4. More information on the NetStumbler Forums and other online WarDriving Communities is presented in Chapter 8 of this book.

**Figure 1.4** Results of the NetStumbler Forums Poll about Warchalking

| Do you warchalk? You have already voted on this poll. | | | |
|---|---|---|---|
| Yes | | 0 | 0% |
| No | | 48 | 100.00% |
| | Total: | 48 votes | 100% |

# The Truth about WarDriving

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.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 7



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. In Chapter 10, a step-by-step guide to enabling the built-in security features of these access points is discussed.

## 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 understanding the difference between WarDriving, a legal activity, and theft, an obviously illegal activity.

# Tools of the Trade or "What Do I Need?"

This section will introduce you to all of the tools that are required in order to successfully WarDrive. There are several different configurations that can be effectively used for WarDriving, including:

- Getting the hardware
- Choosing a wireless network card
- Deciding on an external antenna
- Connecting your antenna to your wireless NIC

The following sections discuss potential equipment acquisitions and common configurations for each.

## Getting the Hardware

You will need some form of hardware to use with your WarDriving equipment. There are two primary setups that WarDrivers utilize:

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 8



- The Laptop Setup
- The PDA Setup

## The Laptop Setup

The most commonly used WarDriving setup utilizes a laptop computer. To WarDrive with a laptop, you need several pieces of hardware (each of which is discussed in detail in this chapter) and at least one WarDriving software program. A successful laptop WarDriving setup includes:

- A laptop computer
- A wireless NIC Card
- An external antenna
- A pigtail to connect the external antenna to the wireless NIC
- A handheld global positioning system (GPS) unit
- A GPS data cable
- A WarDriving software program
- A cigarette lighter or AC adapter power inverter

Because most of the commonly used WarDriving software is not resource intensive, the laptop can be an older model. If you decide to use a laptop computer to WarDrive, you need to determine the WarDriving software you plan to use as well. For instance, if you do not feel comfortable with the Linux operating system, you will have to rely on tools that are supported in a Microsoft Windows environment. Because NetStumbler only works in Windows environments (and Kismet only runs on Linux), your choice of software is limited. A typical laptop WarDriving setup is shown in Figure 1.5.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 9

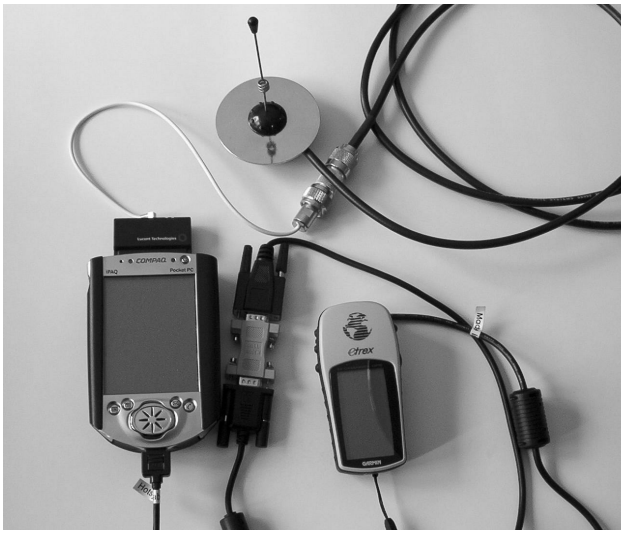


**Figure 1.5** A Typical Laptop Computer WarDriving Setup


## The Personal Digital Assistant (PDA) Setup

PDAs are the perfect accessory for the WarDriver because they are highly portable. The Compaq iPAQ (see Figure 1.6), or any number of other PDAs that utilize the ARM, MIPS, or SH3 processor can be utilized with common WarDriving software packages. See Table 1.1.

**Figure 1.6** A Typical PDA WarDriving Setup



291_WarDriving_01.qxd 2/12/04 11:42 AM Page 10



**Table 1.1** PDA Processors

| Manufacturer/Model | Processor |
|---|---|
| Compaq/Hewlett Packard iPAQ PDAs | ARM |
| Hewlett Packard Jornada PDAs | SH3 |
| CASIO PDAs | MIPS |

As with the laptop setup, the PDA setup requires additional equipment in order to be successful:

- A PDA with a data cable
- A wireless NIC Card
- An external antenna
- A pigtail to connect the external antenna to the wireless NIC
- A handheld global positioning system (GPS) unit
- A GPS data cable
- A null modem connector
- A WarDriving software program

Similar to the laptop configuration, the software package you choose will affect your choice of PDA. MiniStumbler, the PDA version of NetStumbler, works on PDAs that utilize the Microsoft Pocket PC operating system. The HP/Compaq iPAQ is one of the more popular PDAs among WarDrivers that prefer MiniStumbler. WarDrivers that prefer to use a PDA port of Kismet are likely to choose the Sharp Zaurus since it runs a PDA version of Linux. There are also Kismet packages that have specifically been designed for use on the Zaurus.

## Choosing a Wireless Network Interface Card

Now that you have chosen either a laptop or a PDA to use while WarDriving, you will need to determine which wireless NIC card to use. Most of the wireless networks that are currently deployed are 802.11b networks. You will find more access points if you use an 802.11b NIC. 802.11g access points, which transfer data at nearly five times the speed of 802.11b (54 MBps as opposed to 11 MBps) are gaining popularity and it is likely that an 802.11g card will soon supplant an 802.11b card as the favorite of WarDrivers. This is not likely to happen, however,

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 11



until WarDriving tools catch up and offer more extensive 802.11g support. In addition to increased speed, the 802.11g standard supports WiFi Protected Access (WPA) encryption. Once effectively deployed, WPA will help to improve the overall security posture of wireless networks. Some 802.11a cards are currently supported by WarDriving software under certain conditions. These conditions will be discussed throughout the book; specifically in Chapters 2 through 6.

As a general rule, 802.11a (or any 802.11a/b/g combo) cards are not recommended for WarDriving. This is because 802.11a was broken into three distinct frequency ranges: Unlicensed National Information Infrastructure (UNII)1, UNII2, and UNII3. Under Federal Communications Commission (FCC) regulations, UNII1 cannot have removable antennas. Although UNII2 and UNII3 are allowed to have removable antennas, most 802.11a cards utilize both UNII1 and UNII2. Because UNII1 is utilized, removable antennas are not an option for these cards in the United States.

When Kismet and NetStumbler were first introduced, there were two primary chipsets available on wireless NICs: the Hermes chipset and the Prism2 chipset. Although there are many other chipsets available now, most WarDriving software is designed for use with one of these two chipsets. As a general rule NetStumbler works with cards based on the Hermes chipset. Kismet, on the other hand, is designed for use with cards based on the Prism2 chipset. This is not a hard and fast rule since some Prism2 cards will work under NetStumbler in certain configurations. Also, with appropriate Linux kernel modifications, Hermes cards can be used with Kismet.

## Types of Wireless NICs

In order to WarDrive, you will need a wireless NIC. Before purchasing a wireless card, you should determine the software and configuration you plan to use. NetStumbler (see Chapters 2 and 3) offers the easiest configuration for cards based on the Hermes chipset (for example, ORiNOCO cards). NetStumbler offers support for the following cards:

- Lucent Technologies WaveLAN/IEEE (Agere ORiNOCO)
- Dell TrueMobile 1150 Series
- Avaya Wireless PC Card
- Toshiba Wireless LAN Card
- Compaq WL110

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 12



- Cabletron/Enterasys Roamabout
- Elsa Airlancer MC-11
- ARtem ComCard 11Mbps
- IBM High Rate Wireless LAN PC Card
- 1stWave 1ST-PC-DSS11IS, DSS11IG, DSS11ES, DSS11EG
- Some Prism2-based cards will work under Windows XP.

Kismet (described in detail in Chapters 4 through 6) works with both Prism2- and Hermes-based cards. However, most Linux and BSD distributions require kernel and driver patch modifications and recompiles in order for Hermes-based cards to enter monitor mode as required by Kismet. Kismet offers support for the following cards:

- Cisco
  1. Aironet 340
  2. Aironet 350
- Prism 2
  1. Linksys
  2. D-Link
  3. Zoom
  4. Demarctech
  5. Microsoft
  6. Many others
- ORiNOCO
  1. Lucent ORiNOCO-based cards such as the WaveLAN
  2. Airport
- AIRPORT
  1. Airport cards under Mac OS X using the Viha drivers
- ACX100
  1. Dlink 650+

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 13



In order to maximize your results, you will want a card that has an external antenna connector (Figure 1.7). This will allow you to extend the range of your card by attaching a stronger antenna to your WarDriving setup.

**Figure 1.7** ORiNOCO External Antenna Connector

Many WarDrivers prefer the ORiNOCO Gold 802.11b card produced by Agere or Lucent (see Figure 1.8) because it is compatible with both Kismet and NetStumbler and because it also has an external antenna connector. This card is now produced by Proxim and no longer uses the Hermes chipset, nor does it have an external antenna connector. The Hermes-based card is still available; however, it is now marketed as the "ORiNOCO Gold Classic."

**Figure 1.8** The ORiNOCO Gold Card

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 14



I highly recommend the ORiNOCO Gold (now the Gold Classic) card. This card is outstanding for both everyday use and for WarDriving. Also, as previously noted, this card can be configured for use in both NetStumbler and Kismet. This is particularly useful when using a laptop computer that is configured to dual boot both Linux and Windows. This allows you to utilize the wireless NIC in both operating systems as well as most common WarDriving software in both environments without having to change hardware.

## Other Cards

Cisco Aironet 350 Series (see Figure 1.9) cards provide a unique functionality in that some models are available with two external antenna connectors. This is particularly useful in areas with tall buildings because you can attach two directional antennas and manually sweep them up and down buildings on both sides of the road at the same time. (Note: this will probably require two passengers to operate the antennas.)

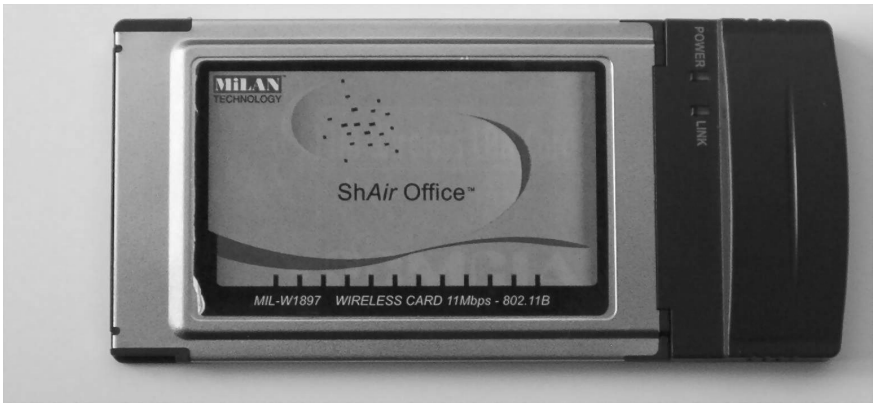
**Figure 1.9** Cisco Aironet 350 Series Card with Dual MMCX Connectors


The "store bought" cards that you find at most major retailers (Linksys, SMC, and so forth) are generally not good cards to use while WarDriving because they do not have external antenna connectors. Most of these cards are based on the Prism 2 chipset (see Figure 1.10).

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 15



**Figure 1.10** A Prism2-Based Card

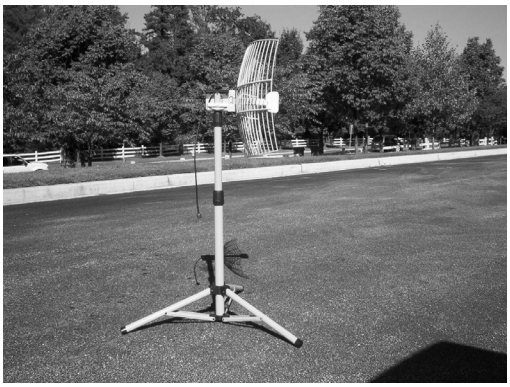



A slightly out-of-date, but still useful listing of wireless NICs, and the chipsets they use was put together by Seattle Wireless and can be found at: www.seattlewireless.net/index.cgi/HardwareComparison.

## External Antennas

In order to maximize the results of a WarDrive, an external antenna should be used. An antenna is a device for radiating or receiving radio waves. Most wireless network cards have a low power antenna built in to them. An external antenna will increase the range of the radio signal detected by the wireless network card. Many different types of antennas can be used with wireless NICs: parabolic antennas, directional antennas, and omni-directional antennas are just a few. Because of their size, parabolic antennas (see Figure 1.11) are not overly practical antennas for WarDriving.

**Figure 1.11** A Parabolic Antenna Isn't Good for WarDriving



291_WarDriving_01.qxd 2/12/04 11:42 AM Page 16



Many WarDrivers use either an external omni-directional antenna or an external directional antenna in conjunction with their wireless network card. Both of these are available in many different sizes and signal strengths. There are many factors that need to be considered when determining what type of antenna to use. This book will not cover specific in-depth details on radio and antenna theory, but will provide some basic information on how antennas work. There are numerous references both online and in print that go into radio and antenna theory in depth.

## NOTE

If you are interested in a more than basic, user-level understanding of the previous concepts, you should investigate the following two resources, *Building a Cisco Wireless LAN* (ISBN: 1-928994-58-X) and *Designing a Wireless Network* (ISBN: 1-928994-45-8), both available from Syngress Publishing (www.syngress.com). Other books include *Jeff Duntemann's Drive-By WiFi Guide* (Paraglyph Publishing, ISBN: 1-932111-74-3), *802.11 Wireless Networks: The Definitive Guide* (O'Reilly & Associates, ISBN: 0-596001-83-5).

The Amateur Radio Relay League (www.arrl.org) also provides some excellent information on antennas and antenna theory. Although this information is geared primarily toward amateur, or HAM, radio, the theories presented are the same regardless of the radio spectrum you are transmitting in.

There are some basic terms you should understand when determining what type of antenna should be used while WarDriving:

- **Decibel (dB)** A decibel is the unit of measure for power ratios describing loss or gain, normally expressed in watts. A decibel is not an absolute value—it is the measurement of power gained or lost between two communicating devices. These units are usually given in terms of the logarithm to Base 10 of a ratio.
- **dBi value** This is the ratio of the gain of an antenna as compared to an *isotropic* antenna. The greater the dBi value, the higher the gain. If the gain is high, the angle of coverage will be more acute.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 17



- **Isotropic antenna** An isotropic antenna is a theoretical construct that describes an antenna that will radiate its signal 360 degrees to cover the area in a perfect sphere. It is used as a basis by which to describe the *gain* of a real antenna.
- **Line of sight** Line of sight is an unobstructed straight line between two transmitting devices. You will most often see the need for a line of sight path for long-range directional radio transmissions. Due to the curvature of the earth, the maximum line of sight for devices not mounted on towers is six miles (9.65 km).

## Omni-Directional Antennas

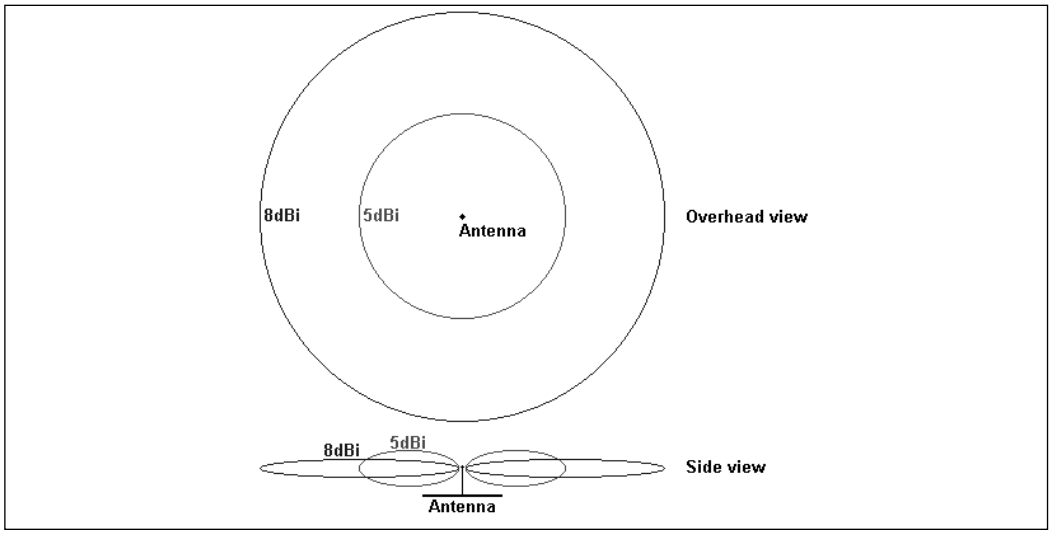
As the name indicates, omni-directional antennas "see" in all directions at once. An omni-directional antenna is best used when driving alone, and can be purchased for $50.00 and up depending on the gain and mounting mechanism. One common misconception is that the stronger the gain of the antenna, the better your WarDriving results will be. This is not entirely true, however. The important thing to understand from the preceding definition of dBi value is the last sentence: "If the gain is high, the angle of coverage will be more acute." Because the signal of an omni-directional antenna is shaped roughly like a donut, the higher (or larger) the gain, the "shorter" the donut. The opposite is true as well. A smaller gain antenna has a "taller" donut.

Figure 1.12 shows the signal donut of a 5 dBi gain omni-directional antenna (see Figure 1.10) compared to that of an 8 dBi gain omni-directional antenna. The signal donut of the 5 dBi is taller than the signal donut of an 8 dBi gain omni-directional antenna. This is illustrated in the side view. What this means is that although it has a "weaker" signal, as indicated in the overhead view, a 5 dBi gain omni-directional antenna is likely to provide better results in a neighborhood with tall buildings such as an urban downtown area. Also, because these antennas rely on line-of-sight communication, a 5 dBi gain antenna works very well in residential areas where homes and other buildings provide obstructions between your antenna and any wireless access points.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 18



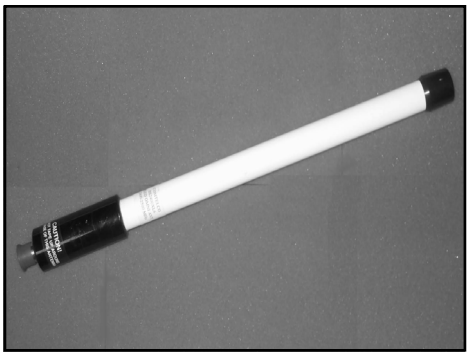
**Figure 1.12** Signal Donut Comparison of 5 dBi and 8 dBi gain Omni-




Another advantage of the 5 dBi gain antenna is that many are available with a magnetic base. This means that you can simply put it on the roof of your car and the magnet will hold it in place while driving; no additional mounting brackets are required.

An 8 dBi gain (see Figure 1.13), or higher, antenna is excellent for use on longer drives in open areas with few obstructions such as interstate highways. These antennas are very effective when businesses or residences are farther away from your vehicle and there is a large field or roadway between you and any potential access points. It is more difficult to find magnetic mounted antennas that are stronger than 5 dBi gain (see Figure 1.14). These antennas usually require some form of external mounting bracket.

**Figure 1.13** An 8 dBi Gain Omni-Directional Antenna



291_WarDriving_01.qxd 2/12/04 11:42 AM Page 19



**Figure 1.14** A 5 dBi Gain Magnetic Mount Omni-Directional Antenna


Regardless of the dBi gain antenna you use, an omni-directional antenna is usually going to be the best choice for WarDriving. This is primarily because it radiates its signal in all directions at once. Because these antennas do rely on line-of-sight communications, it is not necessary to continually sweep the antenna in the direction of potential access points in order to discover them. There are, however, situations where a directional antenna is more effective.

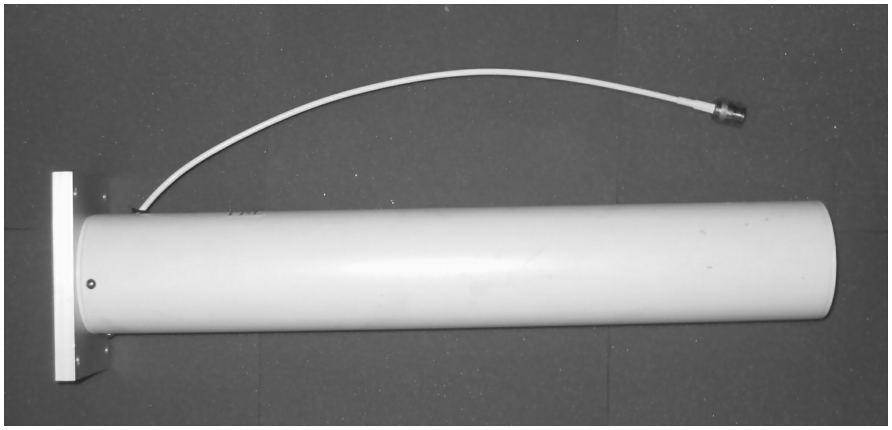
## Directional Antennas

Directional antennas also rely on line of sight to transmit; however, unlike omni-directional antennas, they can only "see" in the direction they are pointed. Directional antennas are excellent for use in areas with tall buildings. From a stationary position near the base of the building, you can sweep the antenna up and down the length of the building and detect access points that would have been missed with an omni-directional antenna. Additionally, directional antennas can have a much stronger dBi gain in a shorter (not necessarily smaller) package. For example, a 14.5 dBi gain directional antenna, as shown in Figure 1.15, is just slightly longer than the 8 dBi gain omni-directional antenna shown in Figure 1.13, but has a significantly stronger dBi gain.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 20



**Figure 1.15** A 14.5 dBi Gain Directional Antenna



There are several types of directional antennas such as yagis, parabolic grids, and so forth. However, the most commonly used antenna is the yagi antenna since these can be purchased relatively inexpensively and provide a large dBi gain.

Notes from the Underground…

## The Pringles "Cantenna"

One of the most fun things you can do is build your own antenna. With a small investment (usually less than $10), you can build a very strong directional antenna. Although this will probably not be an antenna that you will use extensively for WarDriving, taking the time and effort to build your own antenna can teach you many concepts of antenna theory that will be very useful when determining the type of antenna you want to use while WarDriving.

There are a number of online resources that detail the step-by-step methodology for building a "homebrew" antenna. Probably the best is Rob Flickenger's guide at www.oreillynet.com/cs/weblog/view/wlg/448.

The first thing you will need is a hollow cylindrical object such as a Pringles can (emptied of course), a coffee can, an old soup can, or anything with a similar shape. This will provide the housing for the second piece of the antenna, the collector rod. You will need to build the collector rod from parts you can purchase at any Radio Shack.

Continued

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 21



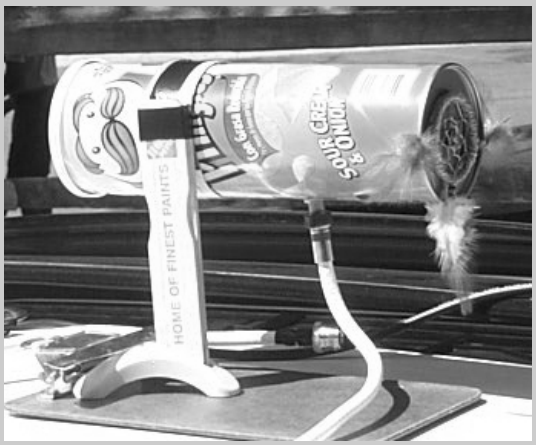
The most interesting part of the process is determining the length of the collector rod. This is where you will learn the most. The basic formula is:

W = 3.0 * 10^8 * (1 / LEF) * 10^-9

In this equation, W is the wavelength frequency and LEF is the Low End Frequency of the channel the antenna should transmit on. Because 802.11b transmits in channels 1–11 of the 2.4 GHz spectrum, if you use the channel 1 LEF of 2.412 and the channel 11 LEF of 2.462, you can determine both the longest (channel 1) and shortest (channel 11) rod you will need. Unless you want the antenna to specifically work on one channel, a much more exacting process, you can keep your rod length between these two values.

After you have determined the longest and shortest wavelength, simply cut your rod to a quarter of those values. In the case of a 2.4 GHz antenna, you will want to keep your rod between 1.2" and 1.22". Once the rod is cut, it is merely a matter of assembling the components and trying it out. (See Figure 1.16.)

**Figure 1.16** The Pringles "Cantenna"




Before attempting to make your own antenna, you should be aware of the risks involved. An improperly constructed antenna could destroy any equipment you connect it to. Also, if your antenna rod lengths are calculated incorrectly, you could transmit outside of the allowable 2.4 GHz spectrum and find yourself on the wrong side of an FCC investigation.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 22



## Connecting Your Antenna to Your Wireless NIC

In order to connect your antenna to the external antenna connector on your wireless NIC you will need the appropriate pigtail cable (see Figure 1.17). Most antennas have an N-Type connector but the wireless NIC usually has a proprietary connector. When you purchase your card you should verify with either the retailer or the card manufacturer what type of external antenna connector is built into the card.

**Figure 1.17** Pigtail for Use with ORiNOCO Cards and N-Type Barrel Connectors

Once you have identified the type of external connector your card has, you will need to purchase a pigtail that has both the correct connection for your card as well as the correct N-Type connector. Some antennas ship with male N-Type connectors and others ship with female N-Type connectors. Because the pigtails are expensive (around $30) you should verify whether your antenna has a male or female connector, and purchase the opposite connection on your pigtail. For instance, if you purchase a 5 dBi magnetic mount omni-directional antenna with a female N-Type connector for use with your ORiNOCO Gold card, you will need a pigtail that has a Lucent proprietary connector as well as a male N-Type connector. This will allow you to successfully connect your antenna to your wireless NICs external antenna connector. Since you may have multiple antennas with both male and female N-Type connectors, it might also be a good idea to

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 23



purchase barrel connectors that will allow you to attach your pigtail to either a male or female N-Type Connector.

## Global Positioning System (GPS)

Most WarDrivers want to map the results of their drives. To do this, a portable GPS capable of National Marine Electronics Output (NMEA) is required. Some WarDriving software supports other proprietary formats (such as Garmin). For instance, NetStumbler supports the Garmin format. The Garmin format "reports" your current location to your software every second, whereas NMEA only reports your location once every two seconds. Using the Garmin format increases the accuracy of the access-point locations. Unfortunately, Kismet (and other WarDriving software) only supports NMEA output. By purchasing a GPS capable of NMEA output, you provide yourself with the flexibility to switch between WarDriving software without requiring additional hardware.

When choosing a GPS, several factors should be considered. As mentioned earlier, making sure it is capable of NMEA output is a must. It is also important to find out which accessories come with the GPS unit. For instance, there are several models in the Garmin eTrex line of handheld GPSs. The base model, simply called the eTrex (see Figure 1.18) retails for about $120. This unit has all of the functionality required for a WarDriver and is capable of NMEA output. When you compare this to the eTrex Venture, which retails for $150, the initial indication would be to go with the cheaper model. However, once the accessories included with these two are looked into, you will notice that the Venture comes with the PC Interface cable, whereas the base model doesn't. Because this cable costs about $50, the Venture is a better purchase. In addition to the PC Interface cable, you get additional functionality with the Venture that, while not required for WarDriving, can be fun to play with, all for $20 less.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 24

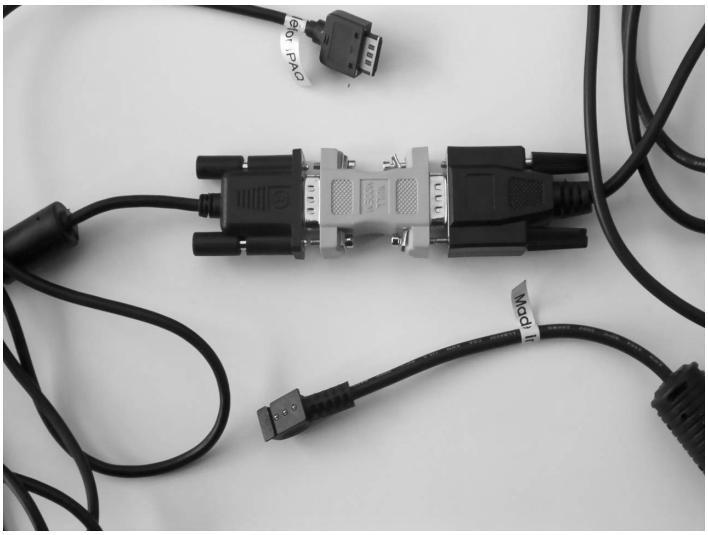


**Figure 1.18** The Garmin eTrex Handheld GPS


You should also determine if your laptop computer has a serial port. Most PC Interface cables have a serial interface. If your laptop doesn't have a serial interface, you can purchase a serial to Universal Serial Bus (USB) cable for use with your GPS.

In order to use your GPS with a PDA, you will need a null modem connector and the proper connection cables for your PDA. The proper configuration for this setup is PDA | Proprietary connector/serial conversion cable | Null Modem Connector | GPS PC Interface cable. This setup is depicted in Figure 1.19.

**Figure 1.19** PDA GPS Cable Connections



291_WarDriving_01.qxd 2/12/04 11:42 AM Page 25



# Putting It All Together

Once you have selected your WarDriving gear and understand what WarDriving is, you are almost ready to begin. You now know that you want to go out and identify wireless access points and map them out, but before you can do this you need to make sure you aren't going to inadvertently connect to one or more of the wireless networks you discover. Because so many access points are set up in the default configuration, this is a real possibility.

Many wireless access points that are available today also include a built-in cable or DSL router to allow multiple hosts to access a single cable or DSL modem and get to the Internet. While this combination does help the end user quickly gain access to the Internet, both on wired and wireless networks, it also increases the potential ways that an attacker can easily compromise the network. This is primarily because, in their default configurations, the wireless access point will allow any card to connect to it without requiring any configuration on the client side, and the router has a Dynamic Host Configuration Protocol (DHCP) server enabled. The DHCP server will automatically assign a valid IP address to any host that requests one from it. When coupled with a wireless access point that grants access to any host, the DHCP server completes the connection process. At this point, an attacker has complete access to all services available on the network.

This is not an issue when using Linux software such as Kismet or AirSnort since these programs operate in monitor mode. A device in monitor mode will merely sniff all traffic without making any connections. In order to avoid accidentally connecting to these networks when using Windows, however, you will need to make a few simple configuration changes before you begin WarDriving. These steps are described in the following section.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 26



### Tools and Traps…

One thing to be aware of when WarDriving is a tool from Black Alchemy called FakeAP (www.blackalchemy.to/project/fakeap/). FakeAP can be configured to generate hundreds or thousands of "fake" access points. A WarDriver that is in range of a system configured with FakeAP will notice a large number of access points quickly being detected. This is because FakeAP generates 802.11b beacon frames with SSIDs and MAC addresses randomly chosen from the FakeAP dictionary.

On a typical WarDrive, it is virtually impossible to detect that access points you have discovered were actually generated by FakeAP. There are several reasons for this. First, by default, FakeAP generates only four fake SSIDs per second. Driving by a system configured with FakeAP is unlikely to register because by the time enough fake access points have been generated for you to notice an anomaly, you will be out of range. Second, FakeAP can be configured to use any dictionary wordlist. This means that the SSIDs will appear to be normal SSIDs. There is no pattern that can be picked out or set of words that can be automatically discounted as FakeAP-generated. Finally, FakeAP can be configured to generate both WEP-encrypted and unencrypted fake access points. In short, this means that because FakeAPs beacons are so random and realistic, it cannot be detected.

In most cases, FakeAP will not be a serious problem for WarDrivers; however, if you happen to get stopped at a traffic light in range of FakeAP, you will have a large number of non-existent access points in your logs that you will either want to remove, or which will cause you to stop your WarDriving application and restart it after you are safely out of range of the system running FakeAP.

## Disabling the TCP/IP Stack in Windows

By disabling the TCP/IP stack in windows, your laptop will not have the functionality to connect to any network. This is a very simple process that you will need to perform before each WarDrive.

1. In Windows 2000/XP, right-click **Network Neighborhood** icon and then choose **Properties**, as shown in Figure 1.20.

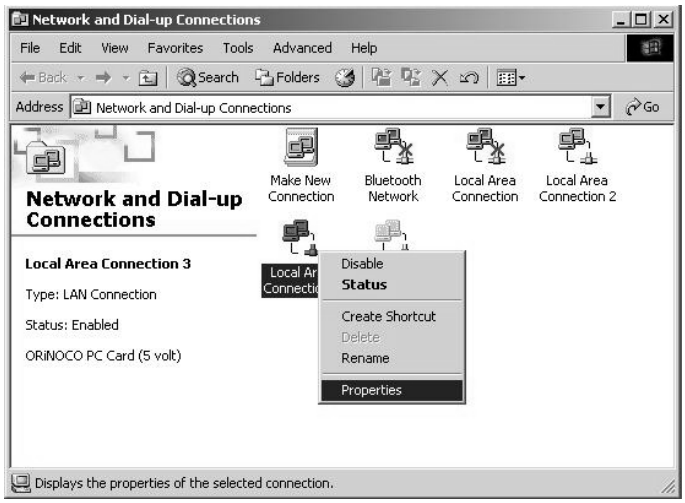
291_WarDriving_01.qxd 2/12/04 11:42 AM Page 27



**Figure 1.20** Disabling the TCP/IP Stack Step One


2. This will open the Network and Dial-Up Configurations window. There may be several network adapters listed here. Locate your wireless network card and right-click it, then choose **Properties** again, as shown in Figure 1.21.

**Figure 1.21** Disabling the TCP/IP Stack Step Two

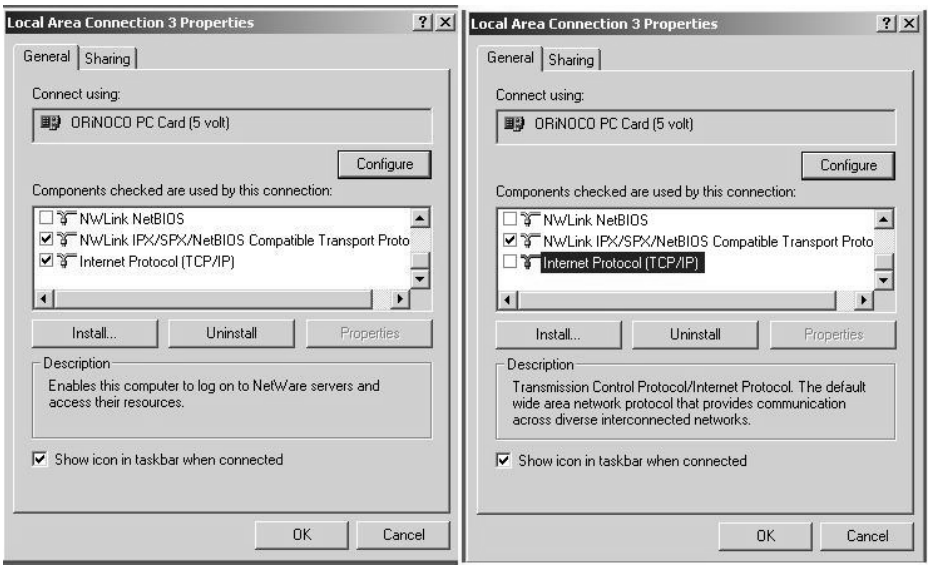



3. This will open the Properties for your wireless network card. Next, simply remove the check from the **Internet Protocol (TCP/IP)** checkbox and then choose **OK**. The before and after views of the dialog box can be seen in Figure 1.22.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 28



**Figure 1.22** Disabling the TCP/IP Stack Step Three




Your TCP/IP stack is now disabled and your wireless network card will not be able to connect to any network. Your WarDriving software will function perfectly even with TCP/IP disabled but you will not expose yourself to possible legal action by inadvertently connecting to a network that you discover while WarDriving. When you are ready to resume normal operations with your wireless network card, simply repeat steps one and two and then replace the checkmark in the **Internet Protocol (TCP/IP)** checkbox and click **OK**.

## Disabling the TCP/IP Stack on an iPAQ

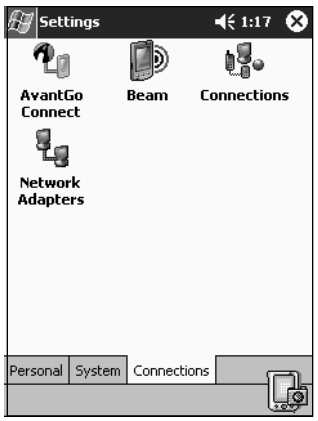
Disabling the TCP/IP Stack on a PDA running Windows CE or Pocket PC is not an option. There is a workaround to this, however; you can set your IP address to a non-routable, non-standard IP address. While this won't absolutely guarantee that you will not connect, it reduces the risk to be virtually non-existent. This is accomplished in three easy steps.

1. Click **Start | Settings** and then choose the **Connections** Tab, as shown in Figure 1.23.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 29

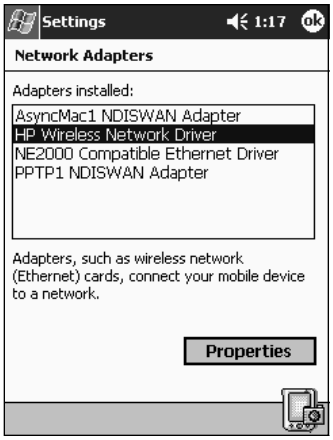


**Figure 1.23** Setting a Non-Standard IP Address on a Pocket PC Step 1




2. Next, click the **Network Adapters** icon. This will bring up a listing of the network adapters that are installed on the handheld device. Select the **HP Wireless Network Driver** and click **Properties** (see Figure 1.24).

**Figure 1.24** Setting a Non-Standard IP Address on a Pocket PC Step 2

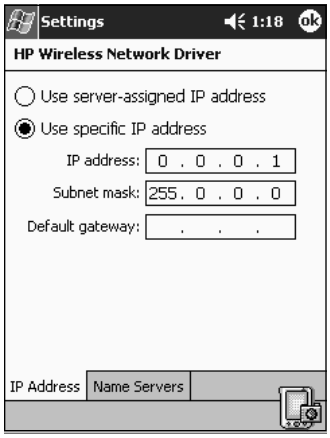



3. Finally, select the **Use Specific IP address** radio button. In the IP address field, set the IP address to **0.0.0.1** and the subnet mask to **255.0.0.0**. Leave the default gateway field blank. Your window should look similar to the window shown in Figure 1.25. Once these values have been set, click **OK**.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 30



**Figure 1.25** Setting a Non-Standard IP Address on a Pocket PC Step 3




After you have clicked **OK**, a pop-up window will appear letting you know that your settings will take effect the next time the adapter is used. Simply click **OK** and then remove and reinsert the PCMCIA card. You can now begin your WarDrive without worrying about connecting to an access point inadvertently.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 31



# Summary

WarDriving, despite the negative connotations that some media outlets have attached to it, is an activity that is not only fun, but that can provide a valuable source of security information to the user community. By WarDriving an area and generating maps and statistical analysis of the security posture of the wireless networks in that region, the residents or businesses there can determine what steps they need to take to secure their wireless networks. Providing this general information can help generate an awareness of the necessity to enable the built-in security measures available on most access points.

If you decide to WarDrive using a laptop computer configuration, you will need to determine the operating system and WarDriving software package you plan to use. Once you have loaded these, you need to insert your wireless NIC card into a PCMCIA slot on your laptop. Next, attach the handheld GPS unit to the serial or USB port on the laptop. Using the appropriate pigtail, connect your choice of an omni-directional antenna, directional antenna, or both to your wireless NIC. If you don't want to run on battery power, connect your laptop computer's power cable to a power inverter. Next, disable the TCP/IP stack if you are using Windows to avoid inadvertent connections to any poorly configured wireless networks. Once all of your connections are in place and you have a power source for the laptop, simply start up your WarDriving software and begin your WarDrive.

Using a PDA setup is a similar process. Insert your wireless NIC into a PCMCIA sleeve for the PDA. Next, attach your external antenna(s) by connecting them to the appropriate pigtail for your wireless NIC. Connect your GPS to its data cable and the serial cable to a null modem connector. Following this, you will need to connect your PDA's proprietary cable to your PDA input slot and the other end to the null modem connector. If you don't want to risk losing power on your PDA in the middle of the drive, you should connect your PDA to a cigarette lighter power source. Next, set your IP Address to 0.0.0.1 with a subnet mask of 255.0.0.0 and no default gateway. Now, simply turn on the PDA and start your WarDriving software.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 32



# Solutions Fast Track

## The Origins of WarDriving

- ☑ WarDriving is the act of moving around a certain area and mapping the population of wireless access points for statistical purposes and to raise awareness of the security problems associated with these types of networks. WarDriving does not in any way imply using these wireless access points without authorization.
- ☑ The term WarDriving refers to all wireless discovery activity (WarFlying, WarWalking, and so forth).
- ☑ The term WarDriving originates from WarDialing, the practice of using a modem attached to a computer to dial an entire exchange of telephone numbers to locate any computers with modems attached to them. This activity was dubbed WarDialing because it was introduced to the general public by Matthew Broderick's character, David Lightman, in the 1983 movie, *WarGames*.
- ☑ The FBI has stated that WarDriving, according to its true meaning, is not illegal in the United States.

## Tools of the Trade or "What Do I Need?"

- ☑ There are two primary hardware setups for WarDriving:
  a. A laptop computer
  b. A Personal Digital Assistant (PDA)
- ☑ In order to WarDrive, you will need:
  a. A wireless network interface card (NIC), preferably with an external antenna connector.
  b. An external antenna of which two types are primarily used:
     i. Omni-directional antennas are used to WarDrive when you want to pick up as many access points as possible in all directions.
     ii. Directional antennas are used to WarDrive when attempting to pinpoint particular access points in a known location or direction.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 33



c. A pigtail with the proper connectors for use in attaching your antenna to your wireless network card.

d. A handheld GPS capable of NMEA output.

e. An external power source such as a power inverter or cigarette lighter adapter is beneficial.

## Putting It All Together

- ☑ When using Windows operating systems, you should disable the TCP/IP stack to avoid inadvertently connecting to misconfigured wireless networks.
- ☑ When using a Pocket PC or Windows CE, you should set a non-standard IP address and subnet mask to avoid inadvertently connecting to misconfigured wireless networks.
- ☑ Because the tools for use in the Linux operating system use monitor mode, no additional configuration is necessary.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 34



# Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form. You will also gain access to thousands of other FAQs at ITFAQnet.com.

**Q:** Since store-bought wireless NICs don't have external antenna connectors, where can I purchase cards that have them?

**A:** Both Wireless Central (www.wirelesscentral.net) and Fleeman, Anderson, and Bird Corporation (www.fab-corp.com) sell cards with external antenna connectors. They also sell pigtails, antennas, and other wireless accessories.

**Q:** What is the difference between using the NMEA standard when WarDriving and the Garmin proprietary standard?

**A:** The NMEA standard reports its signal to your WarDriving software every two seconds. The Garmin standard reports its signal once each second. The Garmin standard can provide a more accurate location for each access point found while WarDriving.

**Q:** Why can't I find an 802.11a PCMCIA NIC with an external antenna connection?

**A:** Because 802.11a cards that are sold today use both UNII1 and UNII2. The FCC has ruled that any UNII1 devices may not be connected to an external antenna. These restrictions obviously apply only in the United States.

**Q:** What are the frequencies used by of each of the 2.4 GHz channels?

**A:** There are 11 channels used in the United States and Canada and 13 channels in Europe on the 2.4 GHz spectrum starting with Channel 1 at 2.412 GHz and incremented by 0.005 GHz for each channel. See Table 1.2 for additional details.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 35



**Table 1.2** Frequency Assignments for 2.4 GHz Band

| Channel | GHz |
|---|---|
| Channel 1 | 2.412 |
| Channel 2 | 2.417 |
| Channel 3 | 2.422 |
| Channel 4 | 2.427 |
| Channel 5 | 2.432 |
| Channel 6 | 2.437 |
| Channel 7 | 2.442 |
| Channel 8 | 2.447 |
| Channel 9 | 2.452 |
| Channel 10 | 2.457 |
| Channel 11 | 2.462 |
| Channel 12 | 2.467 |
| Channel 13 | 2.472 |

**Q:** Both 802.11a and 802.11g networks support speeds of up to 54 Mbps. What is the difference between the two standards?

**A:** There are many differences between the two standards. Two primary ones are that 802.11a operates in the 5.0 GHz spectrum while 802.11g operates in the 2.4 GHz spectrum. Because of the frequency spectrum they're associated with, 802.11g networks support greater distances than 802.11a networks.

**Q:** Are there any good online information resources that WarDrivers should check out?

**A:** User-supported forums are an excellent place to both learn and exchange information with other WarDrivers. Two of the best are the NetStumbler Forums (http://forums.netstumbler.com) and the Kismet forums (www.kismetwireless.net/forum.php). Topics ranging from specific hardware issues to ethics to topical news discussions can be found at both sites.

291_WarDriving_01.qxd 2/12/04 11:42 AM Page 36