Wireless Infidelity I: War Driving

Although WiFi technology security vulnerabilities are well known, the extent of these vulnerabilities may be surprising: War driving experiences identify many potential points of entry.

The concept of wireless networking dates back at least as far as ALOHANET in 1970. While this project is now of primarily historical interest, the online overview is still worth reading (see en.wikipedia.org/wiki/ALOHA_network). The concept of ALOHANET spanned many of the core network protocols in use today, including Ethernet and Wireless Fidelity (aka WiFi). ALOHANET was the precursor of the first generation of wireless networks.

Wireless technologies may be categorized in a variety of ways depending on their function, frequencies, bandwidth, communication protocols involved, and level of sophistication (ranging from first- through third-generation wireless systems). For our purposes, we'll lump them into four basic categories: Wireless Data Networks (WDNs), Personal Area Networks (PANS), Wireless Local Area Networks (WLANs), of which the newer Wireless Metropolitan Area Networks (WMANs) and Wireless Wide Area Networks (WWANs) are offshoots, and satellite networks.

WDN is a cluster of technologies primarily related to, developed for, and marketed by vendors in the telephony and handheld market. This market covers a lot of ground from basic digital cellular phones to relatively sophisticated PDAs and tablet PCs that may rival notebook computers in capabilities. WDN includes protocols such as the Cellular Digital Packet Data (CDPD), an older 19.2Kbps wireless technology that is still in use in some police departments for network communication with patrol cars; General Packet Radio Service (GPRS) and Code Division Multiple Access 2000 (CDMA2000), which are multi-user, combined voice and data 2.5- generation technologies that exceed 100Kbps; and Wireless Application Protocol (WAP), which provides wireless support of the TCP/IP protocol suite and now provides native support of HTTP and HTML. If you're using a cellular phone with text messaging and Web support, you're likely using some form of WAP.

PANs began as "workspace networks." Bluetooth, for example, is a desktop mobility PAN that was designed to support cable-free communication between computers and peripherals. Blackberry (www.blackberry.com) is like Bluetooth on steroids. It integrates telephony, Web browsing, email, and messaging services with PDA productivity applications. As such it blurs the distinction between PAN and WLAN.

WLAN is what most of us think of wireless technology. It includes the now-ubiquitous 802.11 family of protocols, as well as a few others. Table 1 provides a quick overview of some of the 802.11 protocol space. Note that all but the first are derivative from the original

PETER HOEY

802.11 protocol introduced in 1997. In Table 1, "Year" denotes the approximate year of introduction as a standard (for example, 802.11a and 802.11b were introduced at the same time, though 802.11a came to market later). The two bands used for WiFi are Industrial, Scientific, and Medical (ISM) and Unlicensed National Information Infrastructure (UNII). Bandwidth is advertised maximum. Encoding, aka "spectrum spreading" techniques appear at the physical or link layer and include frequency-hopping spread-spectrum (HPSS), direct-sequence spread-spectrum (DSSS), and orthogonal frequency division multiplexing (OFDM).

Both the 802 and 802.11 landscape are somewhat more cluttered than the table suggests. For example, 802 also allows for infrared support at the physical layer. In addition, proprietary standards for 802.11 have been proposed. In 2001, Texas Instruments proposed a 22Mbps variation of 802.11b called "b+", and Atheros proposed a 108Mbps variant of 802.11g called "Super G". Further, there are standards for enhanced QoS (802.11e) and enhanced security (802.11i) that are actually orthogonal to the traditional 802.11 family in the sense that they deal with limitations rather than the characteristics of the protocol suite. To make comparisons even more confusing, there are 802.1x protocols like 802.16 (2001) and 802.16a (2003) that are designed for wider area coverage: the so-called Metropolitan Area Networks or MANs. The 802.11n specifications are meager as of this writing, although the current attention is on increasing throughput at the MAC interface rather than the physical layer.

Standard	802.11	802.11a	02.11b	802.11g	802.11n
Year	1997	1999	1999	2003	2005
Frequency	2.4GHz	5GHz	2.4GHz	2.4GHz	5GHz?
Band	ISM	UNII	ISM	ISM	?
Bandwidth	2Mbps	54Mbps	11Mbps	54Mbps	100+Mbps
Encoding Techniques	DSSS/FHSS	OFDM	DSSS	OFDM	?

Table 1. The 802.11 protocol family.

The Origins of War Driving

The first formalization of the concept of war driving, circa 1999, is attributed to Peter Shipley. His early war driving experimentation was subsequently introduced to the hacker community at DEF-CON 9 in Las Vegas in July 2001; Figure 1 is derived from this experiment.

The basic idea behind war driving is to "sniff" 802.11 traffic with a wireless card set to monitor mode so that it accepts all traffic on a frequency irrespective of intended target. War driving is an extension of the concept of war dialing that deserves some explanation.

War dialing is the technique used by the main character in the 1983 movie *WarGames* to gain access to computer systems. One

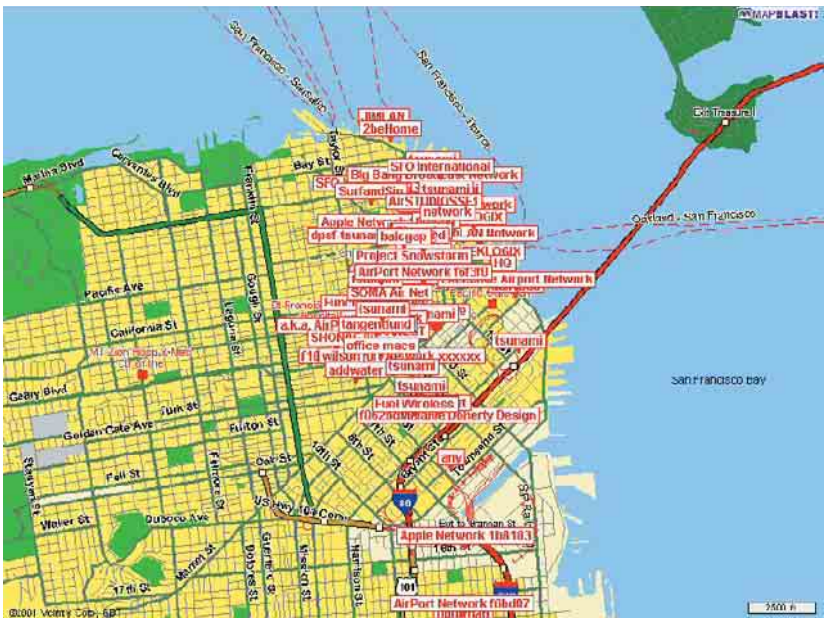

Figure 1. An early WAP map, circa 2001 (source: Peter Shipley, "Open WLANs—The Early Results of WarDriving"; www.dis.org/filez/openlans.pdf).

might recall that in an effort to access computers of a computer game company, the film's main character launched a countdown to a nuclear war. Though modem banks are technological dinosaurs, they remain in use and are one of the easiest network appliances to compromise.

War dialing is the art of scanning lists of phone numbers for the carrier tones that indicate modem lines. The target lists are derived from sundry public-domain sources such as telephone directories (for example, 411.com), WHOIS domain registration Web sites such as Internic (www.internic.net/whois.html), contact information on organizational Web sites, and so forth. The principle is relatively simple: find an organizational telephone number, and then sweep through the range of numbers that includes it for the presence of a modem. A modem's carrier tone signifies a receptive appliance, so the war dialer records a "hit." A suitably enhanced war dialer can "nudge" the unsuspecting modem line to try to produce a logon prompt, and then to produce an acceptable logon sequence. A Web search will confirm that war dialers in both shareware and commercial versions abound for both Windows (THC-Scan 2.0)[1] and *nix (Ward) platforms. At one point, the good folks at l0pht.com even produced a Palm-based war dialer called TBA (see www.securiteam.com/tools/TBA_-_PalmOS_ war-dialer.html).

Figure 2. A "WAP map" of nine WAPs revealing individual coverage areas (source: www.ittc.ku.edu/wlan/images_ittc_small.shtml).

War Driving Takes Shape

There is no question that there is a legitimate, lawful use of war dialing—to determine whether there are insecure modems connected to one's own network. Of course, this knowledge is also of use to potential intruders.

Similarly, war driving is the art of monitoring wireless traffic. The legitimate, lawful use is to control signal strength, bandwidth, leakage patterns, and so forth, for one's own wireless environment. And again, this information is useful to potential intruders.

One thing that distinguishes war driving (aka, WAP mapping, and transportation-centric offshoots like war walking, war biking, war flying, war boating, and the like) is that they all relate to the various modes of mobile sniffing of wireless traffic. Generally speaking, if the sniffing is used in support of the owner/organization's interests, the use of less alarming euphemisms like "wireless monitoring" or "vulnerability testing" is encouraged.

But, let's be candid about this situation: War driving surpasses wireless monitoring by a large measure. To wit, the war drivers have even created their own style of war driving signage known as war chalking that reveals such information as the service set ID, bandwidth, and whether security is enabled. The war chalker identifies the characteristics of the unwitting target on the most convenient visible surface in much the same way the hobo chalkers did during the Great Depression in the U.S.[2] An annual war dri-

[1] The de facto standard for war dialing is THC-Scan 2.0 for Windows. It is available from The Hacker's Choice (www.thc.org). One of many shareware Unix variants is Ward from Securiteam (www.securiteam.com/tools/6T0001P5QM.html).

[2] War chalking follows in the tradition of hobo tagging and tramp signing. A good source of the latter is www.worldpath.net/~minstrel/hobosign.htm. A popular war chalking resource is www. blackbeltjones.com/warchalking/index2.html, the Google top hit, warchalking.org, was not functioning when this column was written in July.

ving competition is held, with results presented at the DEFCON hacker convention every summer (the fourth and most recent competition occurred in June).

	WWWD1 (2002) (9374 WAPs)	WWWD2 (2002) (24958 WAPs)	WWWD3 (2003) (88122 WAPs)	WWWD4 (2004) (228537 WAPs)
Default SSID	29.5%	35.3%	27.8%	31.4%
no WEP enabled	69.9%	72.0%	67.7%	61.6%
Default SSID and no WEP enabled	26.7%	31.4%	24.8%	27.5%

Source: www.worldwidewardrive.org/

Table 2. WorldWide war drives.

The typical war drive reveals a pattern of Wireless Access Points (WAPs), as shown in Figure 2. This information is derived from a wireless detector or computer with a wireless card operating in monitor (RFMON) mode. In the early period of war driving (circa 2000), the war driver's vehicle would have a front seat strewn with cables, antennae, GPS equipment, and a notebook computer. Now, this detection is usually done with a self-contained PDA, with analysis performed offline on a full-screen computer. Figure 3 illustrates the process on a Windows CE-based PDA operating Air Magnet. As the screen in Figure 3 illustrates, the current scan is being performed on channel 6 for 802.11b traffic at 2.4370GHz. The two WAPs detected are reported, along with their MAC addresses, names, and current signal strength. This information is collected and plotted to produce the WAP maps. While this is a cursory overview, it gets to the essence of war driving; I will expand on this topic in a subsequent column.

Figure 3. Wireless "sniffing" Palm style with Air Magnet and a HP IPAQ Pocket PC.

War Driving Lessons

In short, war driving has demonstrated that wireless technology has opened the largest computer network security hole since the advent of modems.

The data in Table 2 comes from the four WorldWide War Driving competitions. By way of background, the Service Set ID (SSID) in Table 2 can be thought of as the "name" that is assigned to a WAP in "infrastructure mode." This name is needed for clients to associate with it. Obviously, the first step toward security is to avoid broadcasting the SSID to the world. The second step is to pick a name that isn't the default set by the vendor. "Default SSID" reports the percentage of the WAPs that were discovered using the SSID that came shrink-wrapped with the WAP hardware.

Wired Equivalent Privacy (WEP) is the encryption technique used in the popular 802.11 protocols. Simply stated, there's little to recommend it as it fails virtually every reasonable standard for data integrity, confidentiality, and authentication in both theory and implementation. While WEP will not withstand a serious attack from any would-be intruder armed with free tools available on the Internet, it will slow down the attacker if properly configured, and will discourage neophytes who seek to authenticate with the WAP. The only thing worse than enabling WEP is not enabling WEP! The data in Table 2 indicates that over 60% of the WAPs detected fail to have WEP enabled. In the wireless realm, this is akin to leaving your wallet on

the front porch for safekeeping.

The worst of all possible worlds is to not employ encryption and at the same time broadcast the name of your WAP to the entire neighborhood and any passersby—approximately 27% of the WAPs found have achieved that status. Most alarming, the percentages do not seem to be changing much over time.

Final Words

The difference between wireless hacking and wireless monitoring is intent and moral orientation. From a technology perspective, they are two sides of the same coin. A similar point is made in an earlier column of mine on Internet Forensics (August 2003). The relevant skill sets of those who attempt to compromise network security and those who seek to protect them are for all practical purposes identical.

Therein lies the rub. The best

URL PEARLS

More information on the originator of the term war driving, Peter Shipley, is available at his Web site: www.dis.org/shipley/. Details of his presentation at Defcon 9 in 2001 are available at ww.defcon.org/html/defcon-9/defcon-9-speakers. html and in "Open WLANs—The early results of WarDriving" at www.dis.org/filez/openlans.pdf. For general treatment of the topic of war driving, visit wardriving.com. A useful definition of war driving is available on Paul McFedries' Word Spy site, www.wordspy.com/words/wardriving.asp. The results of the four International war driving competitions are documented at www.worldwidewardrive.org; information, computer, and network security issues are prevalent at the DEFCON site (www.defcon.org).

Dug Song is one of the world's premier hackers. He founded monkey.org and through it has distributed a suite of very popular tools within both the white hat and black hat communities. Examples include dsniff (a network sniffing utility), fragroute (a generic packet fragmenting tool), the switch state table flooder discussed in this column, and dozens of other tools. In the past few years he has restricted access to some of these resources—see www.linuxsecurity.com/articles/cryptography_article-3624.html, though most remain easy to find via Web search.

WAP mapping is an interesting multimedia exercise in its own right. Figure 2 was produced by the University of Kansas' Wireless Network Visualization Project (www.ittc.ku.edu/wlan/). The coverage maps are particularly revealing from the point of view of wireless leakage. A more general source of "cybermaps" is the Atlas of Cyberspace site at www.cybergeography.org/atlas/.

At this writing, the best wireless detectors I am aware of are Kismet (www.kismetwireless.net) for *nix platforms and Air Magnet (www.airmagnet.com) for Windows.

A useful guide to 802.11 wireless technology is Matthew Gast's *802.11 Wireless Networks: The Definitive Guide*, O'Reilly & Associates, 2002.

More on Alternate Data Streams

I received a good amount of reader correspondence regarding my December 2003 column on Alternate Data Streams and continue to receive feedback months after the issue appeared. Most of the reader comments were sympathetic to the idea that the negative publicity surrounding Window's ADSs is undeserved. If Microsoft is to be faulted, it's for not releasing enough technical documentation to ensure that ADSs can be deployed effectively, efficiently, and securely.

Some readers noted there was an error in the column pertaining to reporting on the Mac OS X lineage. It was incorrectly reported that Mac OS X was built on a Linux kernel; it is actually built on Mach micro kernel derived from FreeBSD. OS X using Apple's HFS+ file system still uses file forks; the alternative UFS (Unix File System) uses .rsrc files instead.

In addition, there was a typographical error in the December column: In the third paragraph, "non-monotonic" should be replaced by "non-monolithic."

Our general-purpose Alternate Data Streams location and editing tool, wantADS, is available as a free download from the Center for Cybermedia Research site at ccr.i2.nscee.edu. C

of breed tools for wireless sniffing (Kismet for the *nix platforms; Air Magnet for Windows) are used by both air jackers and wireless guardians, though toward different ends. This is a familiar story in network security—most of the products developed have benevolent and malevolent uses. (Although Dug Song's switch flooder, Arpspoof, stretches this claim). The lesson to be learned from war driving is that there is nothing inherent in the "sniffing" technology that encourages socially unacceptable or illegal behavior. The tools a hacker might use to intercept organizational wireless traffic are the same tools that are used to harden the organizations' wireless infrastructure.

The solution to the problem of misuse is awareness, both in terms of the capabilities of the tools and the uses toward which they're put. Knowledge and vigilance are formidable adversaries of misuse. I've endeavored to contribute to the former in this column. C

Hal Berghel (www.acm.org/hlb) is a professor and the director of the UNLV School of Computer Science, and director of the University's Center for Cybermedia Research and co-Director of the National Identity Theft and Financial Fraud Research and Operations Center.