

South Florida Sun-Sentinel

COVER

16

SOUTH FLORIDA SUN-SENTINEL • YOUR BUSINESS

Popular wireless networks expose South Florida business's most sensitive data to drive-by hackers.

SNEAK THIEVES

Last spring, **Best Buy** got the kind of publicity no company wants when "wardrivers" went public on a computer bulletin board claiming they were able to see credit card numbers transmitted from a portable

cash register at an unidentified store, just by sitting in a store parking lot with a well-equipped laptop.

**Story by
CHRISTINE WINTER
Business Writer**

The giant retailer immediately took the temporary cash registers out of commission to reassess security, but there were two immediate results: the bad reputation that wireless networks have for poor security was enhanced, and "wardrivers" became part of the public consciousness.

Wardrivers are hobbyists who drive around with laptops with a wireless network access card and an antenna, using free software downloaded from the Internet, to identify the location of wide-open wireless networks.

There probably isn't as much actual wireless hacking — or whacking, as it is called — going on as there is mapping of the open wireless access points by computer savvy kids joyriding with a laptop, looking for free Internet access. And while the wardriving phenomenon has perhaps been overhyped, once your system is identified as being unprotected, your corporate net-

work is at risk and you open yourself to liability if your computer system is used for illegal activities.

The problem today is that many small businesses, while unwilling to share their bandwidth, don't realize they are advertising how easy it is to access their wireless local area networks. They unwittingly broadcast their accessibility by simply plugging in a wireless access point — an easy-to-use, inexpensive device that allows properly equipped mobile devices to communicate with the corporate network — without changing default settings or adding security

precautions.

PROWLING FOR VICTIMS

Wardriving, sometimes called "802.11b-Spotting" for the most commonly used wireless technology, has become a popular tool with security companies to audit their clients' systems, and especially to do drivebys to convince potential customers of their vulnerability.

But it started about a year and a half ago with hackers and hobbyists, mostly kids, who equipped their laptops with a wireless network card, free software from the Internet like Net-Stumbler and Air Snort, and an antenna — perhaps even jury-rigged from an empty Pringles or stew can. Some wardrivers add global positioning system (GPS) cards to their laptops, which even pinpoint the exact physical locations of the unprotected networks, and then post the maps online.

The general consensus among experts is that most wardrivers are simply looking for free Internet access and bandwidth. But the renegade surfers could also launch viruses or spam that could be traced back to the network they accessed, rather than them. And there is the opportunity, once inside the network through that unprotected wireless gateway, to steal or change sensitive data, or even crash the system.

"You may think you are just a small company and no one would want to hack your network, but they may just want to use you as a jumping off point," said Righter Kunkel, senior network security engineer for Fort Lauderdale-based **CyberGuard Inc.**, which makes network firewalls.

First wardrivers find the wireless networks, and then they can use other hacker tools for eavesdropping on the data packets being transmitted by radio waves. Then they can plug this data into other automated software programs that can crack encryption, guess at passwords, and figure out the names and network addresses of servers.

OPEN AND UNPROTECTED

Yet no one is quite sure how

many actual cybercrimes are committed through wireless access, because victims are seldom willing to admit it and much of it is hard to detect. But experts say the potential for mischief, theft or damage once the network is breached is so great the government has recently outlawed wireless connections to classified networks or computers in the Pentagon and much of the military.

The fear is that once wardrivers are inside a network, they may decide to do more than read their own e-mail.

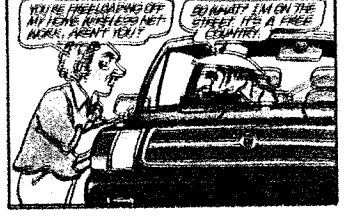
"I've seen cases where kids are just playing around with free Internet access and then they get curious and started wondering, 'Hey, what else is on this network?'" said Ed Skoudis, vice president of security for **Predictive Systems**, a New York-based consulting firm. "Although wireless is not the main attack vector today, it's such a trivially easy way to get in, we expect to see many more wireless attacks in the future."

On a recent stroll through downtown Fort Lauderdale, Christopher Day, chief technology officer at **Asgard**, a Fort Lauderdale network security firm, was able to identify 16 wireless networks in a three-block range of businesses that included retail, restaurants, banks and professional services. Thirteen of these were not using even the most basic security, the wireless encryption system known as WEP (Wired Equivalent Privacy), which has a reputation for being easy to crack.

That's more than 80 percent of wireless users who left themselves open, a figure even higher than the 72 percent of systems found not to be WEP-enabled in a recent national wardriving event, the Second WorldWide WarDrive, held from Oct. 26 to Nov. 2 by wardrivers all over the country to publicize security risks.

While there are programs that can easily break WEP, Day noted it takes a little time and it makes gaining access a little harder. Using it, he suggested, might be enough to lead some intruders to seek an easier location, just as a barking dog can

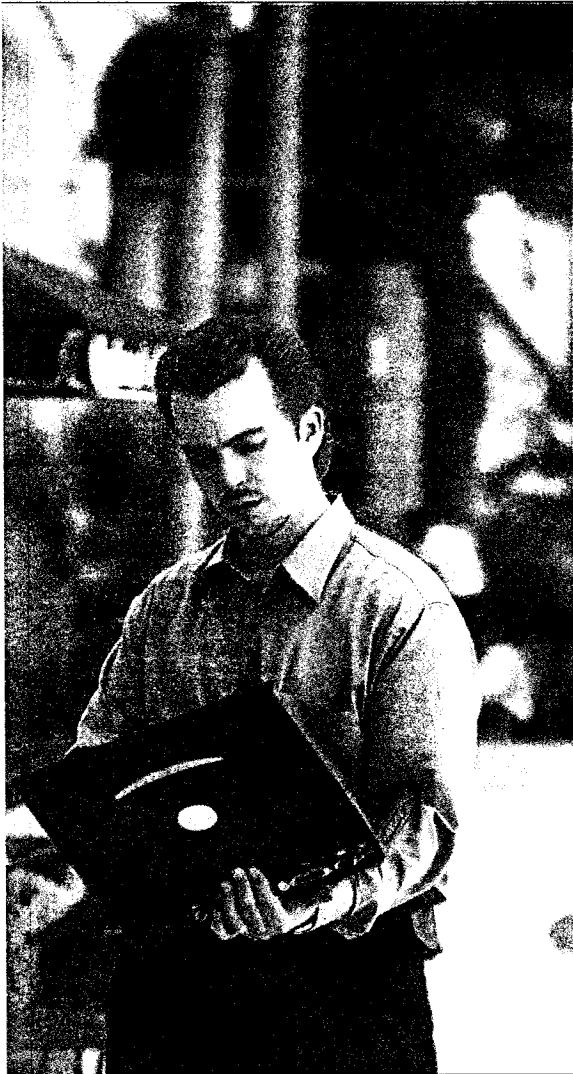
DOONESBURY



sun-sentinel.com

MONDAY, DECEMBER 2, 2002 • BR

STORY



CHECKING IT OUT: Christopher Day, chief technology officer of Asgard Network Security, picks up signals of wireless networks in buildings on Las Olas Boulevard in Fort Lauderdale, indicating the systems' vulnerability to hackers. *Staff photo/Judy Sloan Reich*

eter a burglar.

SECURE SOLUTIONS

Most of the Fort Lauderdale wireless networks had also

failed to change the default setting on the identification code that is broadcast by their systems, and others changed it to include words that gave away their

address or identity, which again, Day warned, makes it easier to find your network and access it.

After identifying the presence of wireless networks, Day then switched to a Linux-based sniffing program that showed streams of data being transmitted, including some IP (Internet Protocol) addresses and an occasional e-mail address or user name, all fodder for automated programs that can crack security and guess passwords. One quickly detected revelation: somebody in the neighborhood was accessing www.fortleatherdale.net, a leather fetishist Web site.

Cyberguard's Kunkel warned about another threat that could be almost as bad as having your own system exposed. "If your network is used to hack another, you might have some liability," he said.

The law is evolving on this issue, according to Bradley Gross, a cyberlaw attorney with **Becker Poliakoff**, based in Fort Lauderdale. However, the national trend is to apply a theory of negligence when an unprotected network is used to attack another computer system or do something illegal such as relay or store kiddie porn, he warned.

Part of the problem is that to get people to accept wireless technology, the devices were designed to be used right out of the box. None of the security is built in as a default, and employees often plug devices in at the office without telling their IT department.

But that doesn't mean that wireless local area networks can't be protected.

"The issue is really not wireless, but the installation and the way it is done," said Tom Ewing, general manager of **Compuquip Technologies Inc.**, a Miami-based systems integrator and monitoring firm.

"Wireless has a bad reputation, but I am confident that if it is set up right, it is extremely secure, even safe enough for a bank to use," he said.

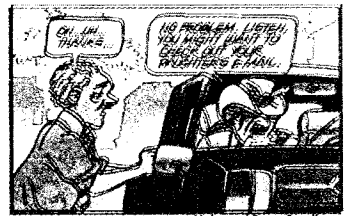
Christine Winter can be reached at cwinter@south-sentinel.com or 954-356-4664.

SECURING YOUR SYSTEM

Here are some tips on how to make your wireless network safer.

- For small businesses and home networks that are not in heavy demand, turn off the wireless access points when not in use. If yours cannot be turned on and off, disconnect the power.
- Try to locate the wireless access point devices toward the center of the facility to minimize the leakage of radio waves to the outside.
- Be aware that most wireless access point devices and cards come with no security configured. Read the documentation on how to turn security features on, and go online to any Web sites provided to update programs to the most current version.
- Educate yourself to the alphabet soup of wireless security: WEP is the most basic wireless security, an encryption system generally considered only moderately safe. A secondary authentication program called LEAP, a proprietary technology from Cisco Systems, can strengthen WEP. A new technology known as Wi-Fi Protected Access (WPA) has been announced by the Wi-Fi Alliance as a replacement for WEP until more robust standards are developed. It should be available early next year.
- If your system allows you to disable the identification code, called an SSID, do it. If not, change it from the default and do not use descriptive words or addresses. This makes it harder for programs like NetStumbler to see who you are. Change any access point passwords set as a default.
- Use MAC-based filters. A MAC address is a unique address given to each wireless network card; authorize your wireless network to accept only those cards with addresses belonging to people you know.
- Treat your wireless network as "untrusted." Place it outside the firewall that protects your corporate network, in an area called a "DMZ," or demilitarized zone, the same way you treat the Internet. If you have high security requirements, install a Virtual Private Network, a system that uses encryption and other security measures to make sure data cannot be intercepted during transmission. However, security experts admit this solution would add cost and complexity to your wireless network.
- If you are using a wireless access point at your office, alert your information technology staff or whoever handles your computer network so they are aware of it. IT managers who say their network is safe because it has no wireless access points are advised to walk around their buildings and look for the simple plug-in devices and antennas.
- If you can't figure it out yourself, hire a professional to spend an hour or two setting up your wireless access point. It might cost as much as \$300, but it is worth it to get it right. Look for technicians who are certified by national security ratings agencies as qualified.
- Remember that the cheapest wireless kits are not always a bargain. Some of the low-priced models cannot be adjusted to make them more secure.

— CHRISTINE WINTER (SOURCES: ASGARD, CYBERGUARD, COMPUQUIP)



Universal Press Syndicate