NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
*A program of the National Institute of Justice*

From Spring 2004 *TechBeat*

TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

# Hot Off the Wireless

*In a recent television commercial a stressed-out office worker takes his laptop to a park and uses his wireless access connection to meet his deadline as he basks in the warm sunshine. Other television and radio advertisements promote the same message: wireless connections make life more convenient, faster, easier. But these commercials do not mention the hidden dangers that every consumer—and every law enforcement officer—should watch for.*

Statistics released by the Federal Bureau of Investigation in 2003 show that "cybercrime" rates increased for the third straight year. Although most people know about financial fraud, identity theft, and the dangers hackers can pose to conventional systems and networks, most are unaware of the unique risks from the use of wireless access technology. Staff at the National Institute of Justice's CyberScience Laboratory (CSL) in Rome, New York, know the risks and want to share this information with law enforcement agencies across the Nation.

Search the Internet for information on wireless technology and you will be overwhelmed by the huge amount of information—some accurate, some not. CSL staff have sorted through that mass of information, applied their technical knowledge and expertise, and produced several primers, an informational DVD, and lists of links to the most useful sites. (These are available by calling the laboratory at 888–338–0584.)

As information technology companies tout wireless use, consumers buy laptop computers and set up wireless access points in their homes and offices without learning about the need for wireless security, says Robert DeCarlo, Jr., an economic crime specialist with CSL. "The vast majority of crimes involving wireless use go undetected and unreported. The victims don't know they're vulnerable, and law enforcement doesn't know the signs to look for. I think we're on the cusp of an explosion of crime using wireless technology."

Jeffrey Isherwood, a CSL senior engineer, says he can recall officers telling him about only one or two cases in which the suspect had wireless access. Ironically, at least half of the officers he talks with tell him they have wireless access in their homes or precincts. Just like the

## A Wireless Intro

**How does wireless access work?**

- Wireless access technology uses radio communication to allow any computer, not only laptops and personal digital assistants (PDAs), to access a network.

**Why use wireless?**

- Wireless connections allow users to access a network from virtually anywhere: home, car, even the beach. They are easy to install and relatively inexpensive to maintain.

**How do you obtain wireless access?**

- Many new laptop computers have built-in wireless adapter cards. These cards also can be purchased at almost any electronics or office supply store. Installation is usually simple: As soon as a user plugs them into a computer, the cards will usually connect to the nearest working access points.

**What are the security risks?**

- It is so easy to set up a wireless local area network (WLAN) that employees may set up access points in their offices without telling their information technology department. Unfortunately, such users may have no knowledge of proper security protocols and procedures.
- All hardware comes with the manufacturer's default settings, which often create access points configured for public access; that is, the newly installed access points are broadcasting "beacon packets" that identify them as available to anyone in the area who is listening. Unfortunately, if cards were manufactured with initial security settings enabled, they might not install easily. Moreover, many users do not know they should immediately reconfigure their access points to restrict access. According to CSL staff,

*Continued on page 2*

average consumer, these officers are aware of the benefits of wireless use, but not its potential security risks. "Wireless often is the last thing that police think of when someone reports identity theft," Isherwood says. "They ask victims where they've been shopping. If they do check victims' computers, they don't think to ask specifically about wireless."

"It's not that there's a specific crime here; it's a method of perpetrating a crime such as identity theft, and it's a method that's very hard to trace and prove," says Joshua Bartolomie, another CSL electronic crime specialist in wireless issues. "For instance, you might live in an apartment building with 10 apartments and someone might be sitting downstairs collecting all of your information. It's the perfect way to perform identity theft."

Bartolomie also says "WarDrivers" (slang for wireless hackers) drive around and look for wireless networks, hoping to find an open access point in a home or office and break into it or piggyback off it from laptops in their vehicles. They break in, cause problems, and then drive away, leaving no evidence behind.

Isherwood says he and Bartolomie perform test sampling whenever they attend a conference. "We use the same equipment and technology that the hackers use," Isherwood says, "and we get numbers that compare to the nationally reported figures. That is, about 75 percent of all wireless access points are unencrypted and wide open, and anybody who wants to can gain access to them."

For that reason, CSL staff caution that officers need to be alert for such warning signs as occupied cars in office parking lots long after businesses have closed, people using laptops in cars, and WarDriving antennas. According to Bartolomie, potato chip cans are almost the exact width and length needed to create an antenna to handle the frequency range that wireless networks use. All a WarDriver needs to create the antenna is another $5 in parts: "If a cop sees someone with a Pringle's can with wires sticking out of it, ask questions!" he says.

"Commercial versions are also fairly cheap," Isherwood says. "They're about 3 inches tall, with a magnetic base. It's hard to distinguish them from a CB or cell phone antenna. Officers should also watch for GPS units and/or laptops connected to the GPS, the antenna, or a can. Anyone using a laptop in a car would arouse my suspicions, period, especially if the car is moving."

"If an officer pulls over someone whom they suspect of WarDriving, he or she should note the time and the license number and report it to whoever in their department handles cybercrime issues. It might prove to be useful information a week, or even a month later, because it might take the victim that long to realize something has happened," he adds.

***A Wireless Intro** (continued)*

although manufacturers provide information about security risks, few people read it.

- Anyone who has the right equipment can detect and break into open access points. Using a potato chip can or a coffee can and some copper wire, an individual can build a directional antenna having a range of hundreds of yards for very little money.

**What basic steps can users take to protect themselves?**

- Wireless access points do not require users to log in with a user name and password. Therefore, IT departments should integrate WLANs into their existing infrastructure to provide maximum protection. Access points should be on a segregated network behind a firewall that requires users to be authenticated before they can access the organization's entire network.
- Wireless fidelity (WiFi) equipment comes with wired equivalent privacy (WEP), a built-in encryption algorithm to scramble data. Although the WEP encryption algorithm can easily be broken, it provides some protection, particularly if users change from the default settings.
- Adding a Virtual Private Network will encrypt an entire framed session, not just the data.
- In a wireless network, Media Access Control (MAC) addresses, which identify network interface cards (each of which has a unique number), can be filtered to provide access to known users only.

**What is WarDriving?**

- WarDriving derives from the term "WarDialing" used in the 1983 movie War Games, in which a teenager used his computer to dial blocks of numbers in search of a way to break into a video game company's systems. It refers to driving, walking, biking, or otherwise cruising around looking for open access points. WarDrivers often use one of many WiFi detection programs available for free from the Internet. Although many WarDrivers do this simply for fun, others have malicious intent. WarDrivers generally need to be within 300 feet of equipment to detect a wireless access point, although if they have high-powered antennas at their disposal, they could be miles away.

**What is the IEEE?**

- The Institute of Electrical and Electronic Engineers (IEEE) establishes standards for wireless use,

*Continued on page 3*

However, these subtle warning signals can be hard to spot. For that reason, CSL staff encourage officers—and consumers—to learn about wireless security and take all the steps they can to safeguard their wireless access. Officers can start by contacting CSL or registering at www.cybersciencelab.com to download *Introduction to Basic Networking, Introduction to the 802.11 Wireless Network Standard,* and *Security Threats to the 802.11 Wireless Network.* These three reports (one of which includes a glossary of basic wireless networking terms) meet the needs of most law enforcement professionals. CSL staff are preparing more advanced documents to supplement these reports.

"We're just interested in getting the information out to State and local law enforcement. If you go to a company website, they're going to plug their products. We're not interested in doing that," DeCarlo says. "We see ourselves as the resource in this area for law enforcement and corrections agencies that need help, and our specialists really know this stuff."

***For more information on wireless access and issues, cybercrime in general, or the CyberScience Laboratory, contact Joshua Bartolomie, 315–838–7057 or Josh@DolphTech.Com; Jeffrey Isherwood, 315–838–7064 or Ish@DolphTech.Com; or Robert DeCarlo, Jr., 315–330–2489 or robert.decarlo@rl.af.mil.***

This article was reprinted from the Spring 2004 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.





including the 802.11 set of wireless access standards. Members of this group of academics and technology professionals work together to adopt and refine protocols and operational standards for many types of community technology.

**What is the 802.11 standard?**

- IEEE has approved three related standards for wireless networking: 802.11a, 802.11b, and 802.11g. (Other standards are in development.) Equipment that meets any of the 802.11 standards falls into the category of WiFi devices. Any equipment carrying the WiFi trademark from the Wireless Ethernet Compatibility Alliance is guaranteed to operate with at least base functionality.
- WiFi uses unlicensed spectrum in the 2.4 GHz range, except for 802.11a, which uses the 5 GHz licensed frequency range. This spectrum originally was left unlicensed so it could be used by microwaves and similar equipment, but many other devices now use this spectrum. The 802.11 standard specifies connectivity at 11 megabits per second (Mbps), compared to 9.6 kilobits per second for older cellular phones. Current phones can connect at hundreds of kilobits per second.
- Most wireless access equipment used in the United States meets the 802.11b standard, operating on a frequency of 2.4 GHz at a maximum speed of 11 Mbps. Devices meeting the 802.11a standard operate at a frequency of 5 GHz at speeds of up to 54 Mbps. Because 802.11b and 802.11a equipment operate on different frequencies, they are not compatible. Devices that meet the 802.11g standard operate at the 2.4 GHz frequency of 802.11b and the 54 Mbps speed of 802.11a; therefore, they are backwards compatible with 802.11b devices. Although all U.S. devices that meet the same standard should work together, this may not be true outside the United States