Originally appeared in the **July 2004** issue of *Communications Technology*.

WI-FI SECURITY

By RON HRANAC

I have a confession to make: I'm a bandwidth thief.

Let me explain.

In the May 4th issue of PC Magazine, columnist John Dvorak discussed unsecured Wi-Fi (wireless fidelity, a term for wireless local area network) access points. Some people drive around looking for open access points so they can get free high-speed Internet access, an activity called wardriving. Dvorak observed that it is illegal in Canada to "steal" bandwidth from open access points, but in the United States the legality of the activity is, as he put it, a bit hazy. Dvorak's position is that it should be the responsibility of the access point owner to secure it and prevent unauthorized persons from using it. He has a point.

After reading the column, I wondered if there were any open access points in my neighborhood. I proceeded to my second floor home office and turned on a Wi-Fi equipped computer, activated its wireless networking feature and waited to see what happened. Lo and behold, the computer identified two access points, one with signal strength in the good category. It was apparent that one of my neighbors seemingly had taken an access point out of its box, connected it to a cable modem and fired things up without changing any of the default settings. Default settings in most, if not all, consumer wireless access points means security is turned off.

I was able to surf the Web easily and check e-mail. So, I guess that makes me a bandwidth thief.

Time for a quick side note. Regular readers know that I dislike using the term bandwidth in reference to data capacity or throughput, although that's how I just used it. Being an old RF guy, I prefer to use bandwidth to denote a specific amount of the electromagnetic spectrum. One could argue that in addition to some of my neighbor's data capacity, I also used a bit of the cable system's RF bandwidth to and from that customer to transmit and receive data. But I digress, as usual.

You might wonder where I'm going with this.

One fairly new line of business for cable operators is home networking. The concept is straightforward: Install a high-speed data customer's home data network—generally for a fee in the range of $100~$200—and maintain it for a few dollars per month on top of the regular cable modem subscription. If something goes wrong with the home network, the cable company fixes the problem. This is a nice source of incremental revenue, and it accommodates the less technically savvy customers who desire home networking capability but have no idea how to install or maintain it.

A home network may be hard wired with Ethernet Category 5 cabling, use a wireless access point or some combination of the two. The issue here is use of wireless access points, whether installed by the cable company as part of a comprehensive home networking installation and maintenance plan, or installed by the customer. We should be encouraging our high-speed data customers to use available access point security features.

Turn on security

As I mentioned earlier, consumer-grade wireless access points are shipped with security settings turned off, supposedly to simplify installation and operation. Unfortunately, most folks don't read the instruction manual and might only skim the quick start guide. The usual drill is to take the access point out of the box, connect it to the cable modem, plug it in to a convenient power source and wireless high-speed Internet access is up and running!

It's difficult to argue with the convenience of wireless Internet access. A Wi-Fi enabled laptop, for instance, can be used for Internet access just about anywhere in the home, without the need for Cat 5 cabling to be pulled through crawl spaces, attics or walls. The obvious downside to running an access point in the clear is that anyone able to receive the access point's signal also can enjoy this convenience, even if that person is sitting in a car outside in the street, or is in the house next door or across the street. Persons with less-than-honorable intentions could use the open access point to launch denial-of-service attacks, send viruses and do other nasties, all without the access point owner knowing what was going on. Indeed, some illegal activities might be traced back to the unsuspecting access point owner!

All of this can be prevented, or at least made much more difficult, by using the access point's built-in security features. Before doing that, however, make sure the access point is running the manufacturer's latest firmware and update it if necessary. Here's a quick summary of things to do to secure most access points. Refer to the manufacturer's documentation for specific instructions and a summary of what security features are supported.

Security checklist

Enable encryption. Most access points support wired equivalent privacy (WEP), which is able to be hacked—even the 128-bit variety, but this will keep honest people honest and is better than no encryption at all. If the access point and PC operating system support it, use the newer Wi-Fi Protected Access (WPA).
Change the default service set identifier (SSID). This is essentially the name of the wireless network.
Disable SSID broadcasts.
Change the access point's default administrative password.
Place the access point near the center of the home or building rather than near an outside wall or window.
Set up a media access control (MAC) address list. This is a table of network interface cards (NICs) or Wi-Fi enabled PCs that are authorized to use the access point.
Consider turning off the access point's dynamic host configuration protocol (DHCP). Instead, assign static Internet protocol (IP) addresses.

Ron Hranac is technical leader, HFC Network Architectures, for Cisco Systems, and former senior technology editor for *Communications Technology*. Reach him at rhranac@aol.com.