Wireless Networking–Security

*Michael J. Ackerman, Ph.D.**

It is the sign of the times: "Wireless Hotspot." You find it in airports, hotels, shopping centers, and coffee shops. It is a location where you can obtain wireless access to the Internet. Sometimes it is free and sometimes there is a charge. Bring your laptop computer with its Wi-Fi adapter (currently 802.11b in most places), and connectivity is yours.

SECURITY ISSUES

Everyone has heard stories about people with laptops parking near corporate office buildings and using the wireless corporate network for accessing the Internet. I have used my neighbor's wireless home network to access the Internet without my neighbor's knowledge or permission. The problem is not piggybacking onto someone else's resource to access the Internet. The real problem is looking at the messages that are flowing across the wireless network or accessing the computers or databases that are attached to that network.

This is not a new problem. It was recognized years ago, associated with the wired telephone system. It was called wiretapping and was made illegal. Voice-scrambling schemes were invented to code sensitive telephone conversations so someone listening in on a wiretap could not understand the words.

. . . hackers can eavesdrop on wired digital transmissions.

In the world of the Internet we must recognize that hackers can eavesdrop on wired digital transmissions. That is why sensitive financial information, such as credit card numbers, are transmitted across the Internet in an encoded fashion. Web sites dealing with financial transactions go into an encoding mode known as the secure socket layer (SSL). You can tell that the Web site is using this secure encrypted mode because the Web address starts with https:// instead of http://.

SSL takes care of Web-based transmissions but may not cover sending and receiving e-mail and associated attachments. Because of this, many companies and government agencies have installed virtual private networks (VPNs). These are schemes that encode transmissions between an employee's computer and the designated Internet service provider (ISP) in such a way that the transmission appears to be crossing a private network, even though it is really crossing the Internet.

. . . virtual private networks (VPNs) . . . are schemes that encode transmissions between an employee's computer and the designated Internet service provider . . .

Each of these techniques was developed to secure information crossing a wired network, a situation where it is assumed that the snooper could make a direct physical connection with the network being tapped. How much easier is it to tap into a wireless network where a physical connection is not necessary and the wireless listening connection is almost trivial to establish and difficult to detect? The designers of the 802.11 family of wireless networks realized this problem and attempted to create solutions in the design of the networks.

When you set up a wireless access point, you must give your network a name, known as the service set identifier (SSID). To connect to the access point, you must supply the SSID. The problem is that the access point broadcasts its SSID. Hackers have created software that can be run on a wireless laptop and that will list all of the wireless signals and their SSIDs available at the location of the laptop. Just click on the SSID and your laptop joins the associated network. Even easier, many wireless network cards designed for use in laptop computers, when told that the SSID to connect to is ANY (all capitals), automatically connect to the strongest wireless signal available.

Wired equivalent privacy (WEP) . . . is an encrypting scheme that was designed theoretically to provide the same level of security as that of a wired network.

Many new access points solve this problem by not broadcasting their SSIDs. The laptop computer must supply the proper SSID to make the connection. The hacker's wireless surveyor or the use of the SSID ANY will no longer work.

*Assistant Director for High-Performance Computing and Communications, National Library of Medicine, Building 38A, Room B1N30, 8600 Rockville Pike, Bethesda, MD 20894; e-mail: mjackerman@earthlink.com.
This article was written by the author in his private capacity. No official support or endorsement by the National Library of Medicine is intended or should be inferred.

It is often said that locks are designed only to keep honest people out. The same may be said for the SSID. The information being transmitted between a laptop and an access point is not encrypted and can be read by a snooper with the proper software within the range of the signal. To address this problem, the designers of 802.11 created wired equivalent privacy (WEP), an encrypting scheme that was designed *theoretically* to provide the same level of security as that of a wired network. Computers in the wireless network and the associated access point are supplied with the same 26-character code made up of the numbers 0 to 9 and letters A to F (techies will recognize this as hexadecimal digits). This code is used to encrypt data while it is in the wireless mode. Unfortunately, hackers were more clever than the network designers. Although breaking the WEP code is not trivial, it is possible with some determined effort—hence, the analogy that locks are designed to keep honest people out.

. . . data are much more secure with WPA encryption than with WEP encryption.

The network designers went back to work. The near-term solution is something called Wi-Fi protected access (WPA). Although it does not totally solve the problem, data are much more secure with WPA encryption than with WEP encryption. WPA is built into many new access points and laptop wireless cards.

The long-term solution is a new data encryption standard called 802.11i. It is designed to work with all of the 802.11 family of wireless networks and is said to supply extremely good security. It will be built into the 802.11 hardware just as WEP and WPA currently are. Look for it sometime next year. Will it be perfect? Just remember that for every lock, there is a key. It's only a question of how difficult it is to reinvent the proper key.

RELEVANCE TO HEALTH CARE

In reference to health care, can a wireless network be used in an office or health-care facility where patient data would cross the network? HIPAA requires that a "reasonable" effort be made to protect patient information.

The long-term solution is a new data encryption standard called 802.11i.

At present, using WEP/WPA encryption and not broadcasting the SSID is the best that can be done and will prevent snooping by all but the most determined thief (including your patients waiting for their appointments). There are no precedents, but most authorities consider this to be "reasonable." When 802.11i becomes available, the definition of "reasonable" will probably include the new standard.

At present, not broadcasting the SSID and using WEP/WPA encryption is the best that can be done . . .

Please keep in mind that connecting a wireless network to the Internet requires the same precautions that connecting a wired network does. Proper security requires a firewall, gatekeeper, and virus software. A "spam sniffer" would also be useful. All this is not that expensive, but you should consult your local Internet security specialist. ■