By Sharon D. Nelson and John W. Simek

Wireless Security for Law Firms©

Editor's Note: We've received a number of questions about the use of wireless communications in law firms. The following addresses some of the security concerns of wireless networks and provides pointers on setting them up securely. For additional information on the 802.11b standard for wireless communications discussed below, see http://grouper.ieee.org/groups/802/11/1st_page.html. Please let us know if you have additional questions you'd like to see addressed in future columns. Questions should be directed to: mbj@mail.michbar.org.

There are many free tools available to "sniff" your data from the wireless airwaves. Besides compromising your data, these tools can be used to see how secure your wireless network really is.

Wireless security…isn't that an oxymoron? The cost for wireless communications continues to come down and implementation is easier and easier to accomplish. Home users, small business, and corporations are all jumping on the wireless bandwagon. Businesses are also marketing wireless "clouds" in their establishments so that you can surf the Internet or gather your e-mail while you're eating a burger or drinking your pedigreed coffee.

The 802.11b standard for wireless communications is the most widely deployed. While there are other wireless standards, most carry the same basic issues regarding security. The 802.11b standard is extremely popular because so many vendors can intercommunicate at this level.

A little lesson in terminology...

There are really only two components needed to effect a wireless connection. The AP (Access Point) is the wireless receiver and connects to your hard-wired network or Internet connection. It is comparable to the base station of your cordless phone. The second device is the computer's wireless network card. This can be an actual card that is installed in a desktop computer, a USB connected device or a PC-Card that goes in a laptop. The wireless card is comparable to the cordless phone itself.

Can you safely use wireless LAN technology in your practice? The simple answer is yes, but be aware of the exposure and changes that you will have to make to your configurations. There are many free tools available to "sniff" your data from the wireless airwaves. Besides compromising your data, these tools can be used to see how secure your wireless network really is.

"War Driving" is where you drive around with your wireless laptop running a sniffing program like NetStumbler (www.stumbler.net), Ethereal (www.ethereal.com) or Kismet (www.kismetwireless.net) and look for wireless "clouds." On a recent drive within Fairfax County (Northern Virginia) of about 14 miles, 99 "hot spots" were discovered. A "hot spot" is where a company has a wireless access point available for connection to their network. We were a little disappointed that we didn't hit the 100 mark, but we reached our destination and didn't have time to continue our search. Of the 99 devices that were identified, only 14 of them had any sort of security enabled. This is a pretty scary statistic considering that anyone could sit in the parking lot of the "hot spot" and gather network data.

Why were so many "hot spots" discovered? Generally, leaving the APs at their default settings will leave you vulnerable to "attack" and hijacking of your network bandwidth. The default settings for many manufacturers' devices are well known and published on multiple Internet sites.

The very first value that should be changed is the password and/or ID that is used to configure and administer the AP. The next thing to change is the SSID (Service Set Identifier). The SSID is a sequence of characters that uniquely names a wireless network. The SSID must match on the AP and wireless network cards in order for a connection to occur. The default SSIDs are well known and make it very easy for someone to connect to your network. When choosing wireless components, pick a vendor

that has the option to disable the advertisement of the SSID. Many manufacturers have the APs advertise their presence so that the network cards can automatically connect right out of the box. The value for the SSID has to match for the network card configuration too, so don't forget to set it on each device that needs to communicate with the AP.

The final modification to help secure your wireless network is to set some form of encryption. Again, the default from the vendor is to transmit all the data in clear text and encryption is not enabled. The simplest encryption to enable is WEP (Wired Equivalent Privacy). Choose the highest encryption level (128-bit) and enter the value in the AP and each wireless network card. There are products that can crack the encryption key such as AirSnort (airsnort.shmoo.com) so be aware of their existence. The practical side is that it takes millions and millions of gathered packets from your network to begin the encryption cracking process. Changing the default values will make this data gathering task much more difficult.

For those truly paranoid about wireless security, just don't install a Wi-Fi network. As an alternative, you can select much more expensive devices where the manufacturer has provided different encryption authentication methods like LEAP (Lightweight Extensible Authentication Protocol) or PEAP (Protected Extensible Authentication Protocol). Another option is to install an 802.11g network as the sniffing and cracking tools aren't designed for these types of networks.

Bottom line: Wireless is here to stay, and we have successfully implemented wireless networks, and secured them as described above, without encountering any security problems. And yes, we do try to break into the very networks we've set up! Where wireless networks are employed, security should remain a constant concern and network administrators should remain vigilant in tracking the development of tools that can crack their networks and in implementing defenses against them. ✦

The authors are the president and vice president of Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax, VA. 703-359-0700 (phone), 703-359-8434 (fax), sensei@senseient.com (e-mail), http://www.senseient.com (website).