Ten Steps to a Secure Wireless Network

IN THIS STORY

- Ten Steps to a Secure Wireless Network

Businesses and home users are quickly adopting wireless networking—and for good reason. It's cheap, convenient, easy to set up, and provides great mobility. In fact, more than one third of *PC Magazine* readers have already installed wireless networks in their homes. The freedom from tangled cables is intoxicating but comes with a price. A wireless network can broadcast far outside your building. With a powerful antenna and some widely available hacking software, anyone sitting near your installation—or even driving by—can passively (without alerting the target) scan all the data flowing in your network.

We pointed out a year ago in "Wireless LANs at Risk" (April 9, 2002) that most wireless setups have no security measures in place. By all accounts, little has changed. But this doesn't have to be the case. Here are ten security techniques you can implement right now.

1. Control your broadcast area. Many wireless APs (access points) let you adjust the signal strength; some even let you adjust signal direction. Begin by placing your APs as far away from exterior walls and windows as possible, then play around with signal strength so you can just barely get connections near exterior walls. This isn't enough, though. Sensitive snooping equipment can pick up wireless signals from an AP at distances of several hundred feet or more. So even with optimal AP placement, the signal may leak. Keep reading.

2. Lock each AP. A lot of people don't bother changing the defaults on their APs, and maintaining the default administrator password (like admin for Linksys products) makes your system a good target. Use a strong password to protect each AP. For tips on creating substantial passwords, go to www.pcmag.com/passwords and click on Password Dos and Don'ts.

3. Ban rogue access points. If an AP is connected to your home or office network, make sure you or the network administrator put it there. Bob in Accounting isn't likely to secure his rogue AP before he connects it. Free software like NetStumbler (www.netstumbler.com) lets you sweep for unauthorized APs.

4. Use 128-bit WEP. Passively cracking the WEP (Wired Equivalent Privacy) security protocol is merely a nuisance to a skilled hacker using Linux freeware like AirSnort (http://airsnort.shmoo.com). Still, the protocol does at least add a layer of difficulty.

5. Use SSIDS wisely. Change the default Service Set Identifiers (SSIDs) for your APs, and don't use anything obvious like your address or company name. For corporate

setups, buy APs that let you disable broadcast SSID. Intruders can use programs such as Kismet (www.kismetwireless.net) to sniff out SSIDs anyway (by observing 802.11x management frames when users associate with APs), but again, every bit of inconvenience helps.

6. Limit access rights. Chances are, not everyone in your building needs a wireless card. Once you determine who should take to the airwaves, set your APs to allow access by wireless cards with authorized MAC addresses only. Enterprising individuals can spoof MAC addresses, however, which brings us to the next tip.

7. Limit the number of user addresses. If you don't have too many users, consider limiting the maximum number of DHCP addresses the network can assign, allowing just enough to cover the users you have. Then if everyone in the group tries to connect but some can't, you know there are unauthorized log-ons.

8. Authenticate users. Install a firewall that supports VPN connectivity, and require users to log on as if they were dialing in remotely. The Linksys BEFSX41 router ($99 list) is a great choice for this. Tweak the settings to allow only the types of permissions that wireless users need.

As a side benefit, VPNs help prevent users from being fooled by malicious association attacks. In this type of assault, the perpetrator sets up a machine that pretends to be an authorized AP, in the hope that someone will be tricked into logging on. If you connect to an AP and don't get the VPN log-on prompt you expect, you know something's amiss.

9. Use RADIUS. Installing a RADIUS server provides another authentication method. The servers tend to be expensive, but there are open-source options, such as FreeRADIUS (www.freeradius.org), for UNIX-savvy administrators.

10. Call in the big boys. If you have billion-dollar secrets to protect, such as the formula to Coca-Cola, you should have wireless-dedicated hardware security in place. For instance, AirDefense (www.airdefense.net) is a server appliance that connects to sensors placed near APs. The system monitors activity and protects all traffic on your wireless LAN—but it doesn't come cheap. Prices start at $10,000 and can reach $100,000 depending on the number of sensors needed.

Wireless Security: WPA Step by Step

IN THIS STORY

By: Craig Ellison

Odds are, your wireless network is not secure. Even if you've enabled WEP (Wired Equivalency Protocol) encryption, the flaws in that standard are well documented, and hackers can break WEP easily. You need WPA (Wi-Fi Protected Access), a far stronger protocol that fixes the weaknesses in WEP. For further discussion of WPA, see our wireless security story.

Here we'll take you through the process of upgrading your networking equipment and enabling WPA security for your home WLAN. To upgrade your wireless security to WPA, you must have three critical components:

- an access point (AP) or wireless router that has WPA support;
- a wireless network card that has WPA drivers available;
- a client (called a supplicant) that supports WPA and your operating system.

WPA replaces WEP in small-office or home routers, so moving to WPA is an all-or-nothing proposition. For you to consider an upgrade, every wireless device on your network must have WPA capabilities. This includes any wireless bridges you might use for your Microsoft Xbox (or other gaming device), digital camera, home audio gateway, and print server.

If you haven't purchased wireless hardware already, buying WPA-capable networking equipment is easy. The Wi-Fi Alliance began certifying products for WPA interoperability in April. In addition, all new products submitted for certification after August 2003 must have WPA capability. Any product that passes Wi-Fi WPA compatibility testing will have the Wi-Fi Protected Access box checked on its package label (Figure 1).

You can also visit the Wi-Fi Alliance's Web site and search for WPA-certified products (www.wi-fi.org/OpenSection/certified_products.asp?TID=2).

If you already own wireless networking hardware, upgrading may not be possible. You must check the Web sites of your hardware makers for WPA upgrades. WPA is

designed so that legacy wireless hardware can be upgraded via drivers, but with the product cycles of wireless gear being about six months, most manufacturers do not provide WPA upgrades for legacy products. If you find WPA support, it will probably be for relatively new products. If you don't find driver upgrades for your hardware, you'll either have to buy new equipment or live with WEP.

For this article, we selected the Linksys WRT54G broadband router and the Linksys WPC54G client card. Both products are widely available and have online driver and firmware upgrades for WPA.