



May 6, 2002

Wireless LAN Security Crackdown

By [Jason Brooks](#)

Cheap and provocative, WLANs are making their way onto production networks through the back door. Tech-savvy employees pick up a system at Circuit City and share the wireless LAN among department colleagues like a box of doughnuts—with about as much thought about the consequences.

The popularity of wireless networking among home and business users alike has kept sales of WLAN equipment strong, even during a weak tech market. In-Stat/MDR estimates that the WLAN market will grow from 3.3 million units shipped in 2000 to 23.6 million units in 2005.

The catalyst for this growth is the dramatic decrease in the price of these systems. Wireless access points based on 802.11b can be had for as little as \$150, and wireless PC Card adapters now cost about \$70 each. What's more, most OEMs now offer laptops with integrated 802.11b radios, and Intel Corp. has announced plans to embed 802.11b support into its forthcoming "Banias" mobile processor.

Tech history is rife with examples of end users (or executive management) leading the charge on gee-whiz technology. Handhelds come immediately to mind as one such case, but WLANs have more inherent security problems—ones that IT managers cannot ignore. IT managers must develop an effective and systemic means of keeping the technology out or a rock-solid plan for building it safely from the ground up. Both approaches require as much policy setting as they do technology deployment.

—Most important, IT departments can't expect that these "rogue" access points will be configured to take advantage of the out-of-the-box security features of 802.11x gear. And even if they are, built-in security such as WEP (Wired Equivalent Privacy) and media access control, or MAC, address lists can still leave WLANs vulnerable to attack.

Almost all 802.11x-based equipment ships with the same basic security measures, each of which has been shown to be vulnerable to attack. WEP encryption, for example, leaves WLANs open to passive hacking attacks that can allow a malicious party to uncover the WLAN's encryption keys by sniffing a given amount of WEP-encrypted wireless traffic.

In addition, unauthorized access points don't have the benefit of the sort of detailed site survey that accompanies a structured WLAN rollout. Companies reduce their WLAN security risks by positioning their access points so their coverage area does not extend beyond the walls of a corporate campus. The casual user is far less likely—if at all—to consider how far the traffic his rogue network is generating will travel.

For the likely well-meaning worker who installs a rogue access point in his or her work space, the most recognizable—and often solely used—security measure is the Service Set Identifier, or SSID.

Each access point is given an SSID, which serves as the name for a given WLAN and which wireless clients must have to access the network. However, most access points broadcast their SSIDs to wireless clients that come looking for them.

In short, whether your company has chosen to deploy a wireless network or not, it is important to draft and implement WLAN policies—even if they only amount to an official policy against installing wireless networking gear at all. IT administrators should distribute this policy, along with an explanation of the risks of insecure WLANs, to all employees of an organization and reinforce regularly.

IT departments can enforce an anti-WLAN agenda by conducting periodic sweeps for rogue access points using wireless sniffer products such as WildPackets Inc.'s AiroPeek NX, Network Associates Inc.'s Sniffer Wireless 4.7 and Network Instruments LLC's Observer 8.1 Wireless Protocol Analyzer. (For a comparative evaluation of these products, go to www.eweek.com/links.)

Although costly—ranging in price from \$3,000 to \$7,000—these products can determine both the presence and location of access points on a corporate campus and make the task of monitoring and maintaining a WLAN much easier. AirMagnet Inc.'s AirMagnet takes a more focused and very effective approach.

Inviting Wireless

While wireless networks are inherently less secure than wired networks, IT organizations that properly build out their WLAN infrastructure can strike an acceptable balance between security and convenience.

Sites that do choose to deploy WLANs can bolster security with VPN (virtual private network)-based solutions such as those from ReefEdge Inc. and SMC Networks Inc. or with vendor-specific applications that patch the gaps in 802.11b.

Many of the larger WLAN vendors, including Cisco Systems Inc., offer complete wireless network implementations that patch the weaknesses in 802.11b security with a mixture of open standards and proprietary hardware and software.

Cisco's WLAN security system depends on the EAP (Extensible Authentication Protocol) extension to RADIUS (Remote Authentication Dial-in User Service) that forces users to log in to an authentication server to access the network. The system provides for mutual authentication between the client and server and generates a WEP key that is specific to the connecting client. This setup eases key distribution issues and helps prevent passive key-sniffing attacks by keeping the keys fresh and unique.

Cisco's solution depends on the proposed 802.1x standard. Microsoft Corp. has built support for 802.1x into its Windows XP operating system, and this will likely help drive adoption.

However, there are many 802.11b-enabled clients, including some handheld computers, that are not equipped to work with these security frameworks. In addition, the client software that these systems require to operate will often work with only wireless adapters from specific vendors.

VPNs to the Rescue

A more flexible and, depending on a company's existing infrastructure, perhaps simpler WLAN security scheme involves VPNs, which encrypt wireless network traffic directly from the access point to the wireless client.

VPN-based systems have the benefit of being platform- and radio- technology-agnostic—that is, the client system establishes a connection to the network via 802.11b, 802.11a or even Bluetooth, and the VPN takes over from there.

This can be particularly attractive to companies that have already developed a VPN infrastructure to secure traffic across a network that's more familiar than a WLAN and equally insecure—the Internet. For a company with a VPN already in place, a WLAN can be situated behind a demilitarized zone that's blocked off from the production network, as in the case of a public Web server. That way, WLAN users may access the Internet through their wireless links but will have to connect to the corporate network—and sensitive network resources—through an encrypted VPN link.

Some operating systems, including Windows 2000, Windows XP and Pocket PC 2002, ship with integrated VPN support, and third-party VPN clients are available for Mac OS, Linux and Palm OS, among others.

While a VPN client does impose some additional processing power overhead—which can prove taxing on handheld devices—we've experienced good performance from the mobile VPN clients we've tested.

Vendors such as ReefEdge and SMC Networks offer gateway appliances that provide turnkey, VPN-based security solutions. ReefEdge's ReefEdge Connect system can authenticate users against an internal database or against a RADIUS, Active Directory or other server and provide for traffic encryption.

Although these systems can be expensive—ReefEdge's appliance starts at \$6,000, for example—they offer enterprises benefits above and beyond security, such as quality-of-service assurance and smooth roaming among access points.

Technical Analyst Jason Brooks can be reached at jason_brooks@ziffdavis.com.

Related Stories:

- [Sniffing Out Rogue Wireless Lans](#)
- [802.11a and 802.11g Evolve the WLAN Space](#)
- **Review:** [AirMagnet 1.2 Reveals WLAN Trouble Spots](#)
- **Review:** [VPN Tools Aid WLAN Security](#)