Understanding Wireless LAN Vulnerabilities

Lisa Phifer

WLAN risks are real—but so are its rewards. Go ahead and install a WLAN, but keep an eye on it

War driving…Air tapping…Drive-by Wi-Fi…. Call it what you will, exploiting the broadcast nature of 802.11 "Wi-Fi" to find and use unprotected networks is fast becoming a national pastime among wireless enthusiasts and hackers.

"War chalkers" leave behind ")(" marks to help fellow road warriors locate unsecured Wi-Fi access points. Frank Keeney, founder of Pasadena Networks, describes his summer vacation of war driving as "making 802.11b wireless access-point mapping fun for the whole family." Garry Trudeau even took a jab at Wi-Fi owners in a recent Doonesbury comic strip. "Man…great hot spot!" exclaims the air tapper. "Why would anyone *pay* for this stuff?"

Unfortunately, to small businesses and large enterprises with wireless LANs, war driving is no laughing matter. Alternately overhyped and underestimated, war driving is the proverbial canary in the coal mine. Getting war-chalked may not mean your network has been exploited, but it should certainly be a wake-up call. Accordingly, this article will discuss some of the myths and realities of WLAN security.

Myth #1: War Driving Is Hard

Some IT administrators naively assume their WLANs are safe. After all, most indoor access points are designed to support users within 300 feet, and because radio waves are easily absorbed by intervening objects—walls, doors, human bodies—the usable network footprint is often frustratingly smaller. Therefore, by placing my Wi-Fi access points (APs) well inside my facility, I should be safe from casual snooping. Right?

Wrong. War driving does not require deep expertise, special wireless cards, beefy PCs or high-gain antennas. Armed with AirMagnet wireless LAN analyzer software, an off-the-shelf Proxim PC card and an HP Jornada personal digital assistant (PDA), I drove along a suburban stretch of the Pennsylvania Turnpike. Moving at 65 mph, with concrete sound barriers and tens of yards separating my car from the nearest building, AirMagnet quickly spotted eight WLAN access points (APs). Half did not have link-level security enabled—including a police department, a physician's office and a pharmacy. How do I know what types of enterprises I was seeing? These WLANs were clearly identified by the network names they were broadcasting.

When I exited the highway and paused at a stoplight, I reached the Internet from the first WLAN I tried to penetrate. The owner of this AP had taken a stab at security. By capturing a few packets, I could see the owner protected his own traffic with ESP (the Encapsulating Security Payload standard used by VPN clients). This AP also did not hand me a valid IP address on a silver platter. However, captured packets were being sent from 192.168.0.3—a private-subnet address used by many gateway and firewall products. I gave my PDA another address in the 192.168.0.0/24 subnet, assumed 192.168.0.1 was the default gateway, and *viola*! I was on the Internet. After sending a few mail messages, I moved on, mission accomplished.

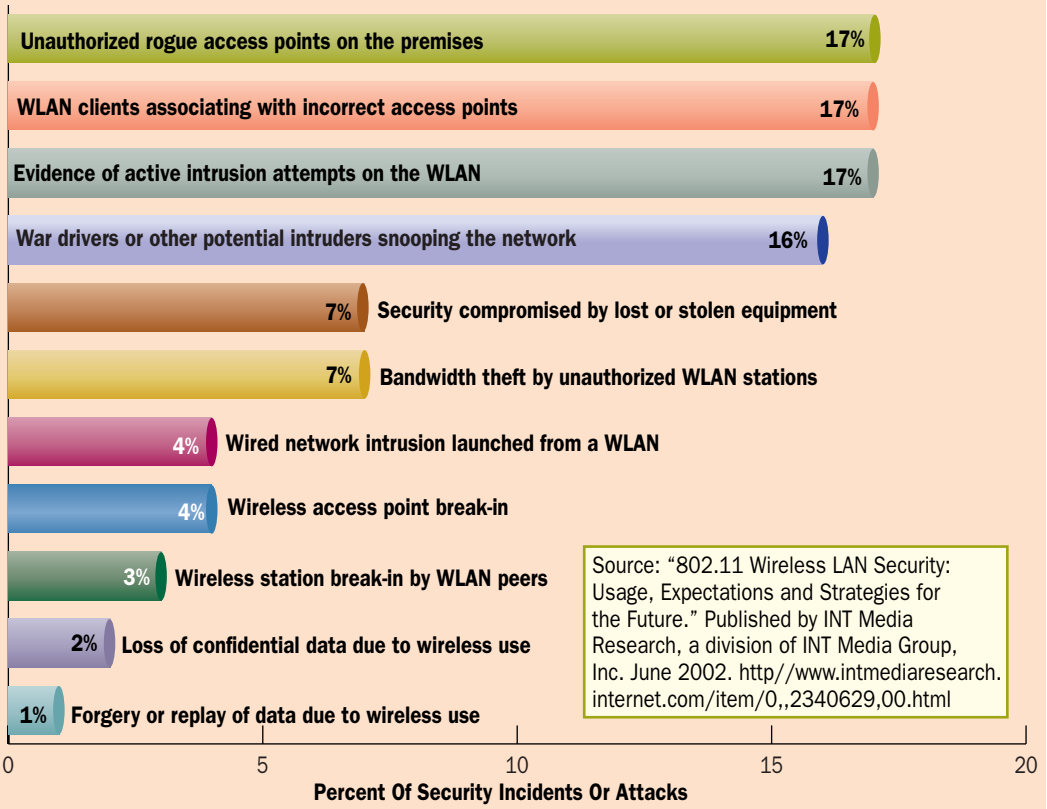
Myth #2: War Driving Is Much Ado About Nothing

In May, Best Buy deactivated wireless point-of-sale terminals after a message board on the website SecurityFocus warned that a customer trying his new Wi-Fi card in the parking lot had seen credit card numbers sent over the air. When similar rumors about Home Depot surfaced, the retailer denied any private data was at risk, since its transmissions are limited to inventory checks and price quotes. When I called the drug store chain I'd spotted in my own travels, CVS, company spokesperson Todd Andrews made a similar statement: "We use wireless strictly for internal item management."

Security is always a balancing act between risk exposure and the cost of eliminating all vulnerabilities. It may be perfectly reasonable to decide that the data being sent over wireless does not require confidentiality. However, even companies unconcerned about eavesdropping should recognize that WLANs may leave another valuable resource—the corporate network—open for unauthorized use.

Lisa Phifer is vice president of Core Competence, Inc., a consulting firm specializing in network and security technologies. She has been involved in the design, implementation, and evaluation of internetworking products for more than 20 years. She can be reached at lisa@corecom.com.

FIGURE 1 Users Reporting WLAN Security Incidents Or Attacks



Source: "802.11 Wireless LAN Security: Usage, Expectations and Strategies for the Future." Published by INT Media Research, a division of INT Media Group, Inc. June 2002. http//www.intmediaresearch.internet.com/item/0,,2340629,00.html

Banning Wi-Fi is usually short-sighted

Unless precautions are taken to isolate WLANs from adjacent wired networks, intranet servers and databases could be breached. Furthermore, owners may be liable for attacks launched by those gaining Internet access through unprotected APs. Attacks could range from relatively benign spam to malicious denial of service (DoS) floods, creating the possibility of both civil and criminal litigation.

Myth #3: If I Can See It, I Can Use It

On the other hand, just because a war driver spots an unprotected AP does *not* automatically mean he or she can reach the wired network behind it. For starters, the war driver needs a valid IP address and gateway into the attached network. Next, outside traffic must get past any MAC filters or user authentication deployed between the open wireless LAN and the adjacent network.

Many WLANs are intentionally left open by enthusiasts who are trying to create a grassroots public infrastructure for wireless Internet access. Not surprisingly, ISPs aren't too enthusiastic about such sharing of connectivity, and the fine print in broadband DSL and cable modem service agreements usually prohibits doing so. For example, in early July, Time Warner sent warning letters to several subscribers known to be using their cable modems to provide wireless public Internet access to others.

Service providers reasonably argue that allowing anonymous access creates a known risk and, therefore, legal liability should an attacker exploit that link. According to Dr. Bill Hancock, chief security officer at Exodus, last year's anti-terrorism Patriot Act raised the stakes even further. Those who own systems that are used to launch cyber-terror-attacks against others can now be prosecuted for aiding in the commission of a terrorist offense.

Myth #4: Wireless Risk Outweighs The Reward

Earlier this year, security concerns led the Lawrence Livermore and Los Alamos National Laboratories to ban the use of Wi-Fi. For most enterprises, such a ban would be short-sighted. A 2001 study commissioned by Cisco reported that using WLANs to improve connectivity to the corporate network saved workers an average of 70 minutes per day.

Another study by The Boston Consulting Group (BCG) claims that companies adopting wireless sales force automation or customer relationship management have increased productivity as much as 30 percent. According to BCG vice president Joe Manget, Home Depot is saving $22 million a year through wireless inventory management. "PepsiCo/Frito-Lay, FedEx and UPS mobilized distribution processes for a cost savings of 10 to 20 percent thanks to productivity gains,

There are several alternatives to operating the WLAN in open mode

increased asset visibility and improved decision-making capabilities," wrote Manget.

Understanding WLAN Vulnerabilities

Shunning wireless LANs now would be akin to banning Internet access a decade ago. Rather, companies should cautiously tap the rewards of Wi-Fi while taking appropriate steps to understand and mitigate associated risks. The first step in managing risk is to fully understand common wireless LAN vulnerabilities.

In a survey that I developed for INT Media Research, Wi-Fi users were asked to identify security incidents experienced by company WLANs over the past year. Not surprisingly, half the participants declined to respond to this sensitive question. Of the remainder, approximately one in six reported at least one incident of unauthorized APs, stations associating with the wrong AP, war driving and active intrusion on the WLAN (Figure 1). As expected, actual penetration into wireless APs, peer stations or adjacent wired networks proved much less common.

Incidents like these illustrate several common WLAN vulnerabilities. To strengthen the security of future WLANs, let us consider the root causes.

Controlling WLAN Access

Undoubtedly, controlling access is more difficult in WLANs than with wireline Ethernet LANs. It's true that nearly every Wi-Fi AP supports Wired Equivalent Privacy (WEP), a link-layer security standard which is intended to make WLANs as "safe" as Ethernet. Yet WEP is relatively weak, and to facilitate plug-and-play networking, most Wi-Fi products default to open system mode. In this mode, there is no access control on the WLAN segment. Any station can join the party simply by sending an "associate" request to the WLAN's AP.

WLANs operating in open system mode have the following vulnerabilities:

- **Unauthorized use of WLAN bandwidth:** All stations sending to an AP eat into the shared bandwidth. Although one 802.11b channel can carry 11 Mbps, overhead typically reduces effective throughput to 6 Mbps or less. Signal strength drops with distance, bottoming out at 1 Mbps. Clearly, WLAN bandwidth is a precious commodity. Even stations without malicious intent that do no more than transmit to your AP still reduce the WLAN capacity available to others.
- **Unauthorized access to intranet services:** Some companies make the mistake of treating WLANs just like Ethernet LANs, deploying APs inside the company firewall. Teleworkers using wireless gateways to reach DSL or cable connections at home often make a similar mistake.

Without adequate access control on the WLAN, wireless gateways and APs should always be placed in untrusted territory. Failure to do so leaves the door wide open for unauthorized stations to access, attack and steal confidential data from intranet servers.

- **Unauthorized access to the Internet:** Even if you firewall your intranet away from your WLAN, what stands between Wi-Fi squatters and your Internet uplink? If your answer is "nothing," unauthorized stations can compete with legitimate users for WAN bandwidth, and your enterprise could be liable for misdeeds launched from your WLAN. MAC- or user-level access controls, deployed on or between the AP and the Internet uplink, can address this vulnerability.
- **Wireless Station Compromise:** Network access control is challenging enough, but what about end stations? Unless desktop security measures are applied, unauthorized wireless stations can hear Windows Network Neighborhood broadcasts, reach shared files or printers or launch denial-of-service attacks against other PCs on the WLAN. Wireless stations must be hardened against peer attack, just like wired PCs with always-on Internet connections.
- **AP Compromise:** The most critical node on the WLAN is the AP itself. Many APs are installed with default parameters—easily-guessed administrator logins, SNMP community strings and HTTP/Telnet listening ports for remote administration. The same methods used to harden WAN access routers should be applied to wireless APs—disable unused services, configure strong passwords and community strings, employ secure management protocols and use access-control lists to narrow exposure. Beware that eliminating these vulnerabilities may not be possible in entry-level APs that lack enterprise-grade security knobs.

Alternatives To Open System Mode

There are several alternatives to operating your AP in open system mode, ranging from simple-but-very-weak to complex-but-more-secure:

- **Closed System Mode:** When associating with an AP, the wireless station supplies the name of the network, called a Service Set ID (SSID). Many APs will accept null or "ANY" SSIDs. Some vendors support an option requiring the station to supply the exact SSID.

By configuring a hard-to-guess SSID, disabling AP beacons that broadcast SSID and enabling *closed system* mode, you can prevent visitors and neighbors from accidentally associating with your AP. However, this will not stop a determined war driver, because SSID values can still be learned by eavesdropping on other frames.

- **Shared Key Authentication:** Most Wi-Fi products support challenge/response authentication using a string (key) known to the station and AP. *Shared key authentication* is simple and can be your first line of defense against casual war drivers. However, it does not provide robust access control. Because shared keys are known to every station, they suffer from group password vulnerabilities. Furthermore, shared keys are static—

manually configured into stations and used for long periods. If the key is disclosed or cracked, recovery takes time and effort. Nonetheless, smaller WLANs—including teleworker WLANs—can benefit from enabling this basic measure.

■ **MAC Access Control Lists:** Most enterprise-grade APs can be configured with MAC address lists that prevent associations with unknown wireless stations. Since you will need a current inventory of MAC addresses, this method requires maintenance and lacks flexibility to authorize very frequent, short-term guest access.

■ **802.1X Port Access Control:** More robust security is available with enterprise-grade APs that support emerging 802.1X standards for port access control (Figure 2). Instead of checking a local MAC list, these APs relay station access requests to a back-end Radius server. If the access request is accepted, a unique key can be supplied to the station to keep session traffic confidential—a better solution than static WEP keys.

The 802.1X standard is a framework based on the Extensible Authentication Protocol (EAP). Implementations vary greatly, depending upon "EAP type." Companies using Windows XP on all wireless stations can deploy 802.1X using a Radius server that supports EAP-TLS (Transport Layer Security), like Microsoft IAS. But EAP-TLS requires a digital certificate on every station.

To simplify station configuration, other vendors have implemented different EAP types—for example, Funk's EAP-TTLS (Tunneled TLS and Cisco's LEAP (Lightweight EAP). By the time you read this, Microsoft, Cisco, Proxim/Agere, and other vendors may support Protected EAP (PEAP), a new EAP type that closes known holes in other types and represents a compromise between major players.

In the long run, most enterprises will control WLAN access with 802.1X. However, standards and implementations must solidify before this approach can see widespread deployment.

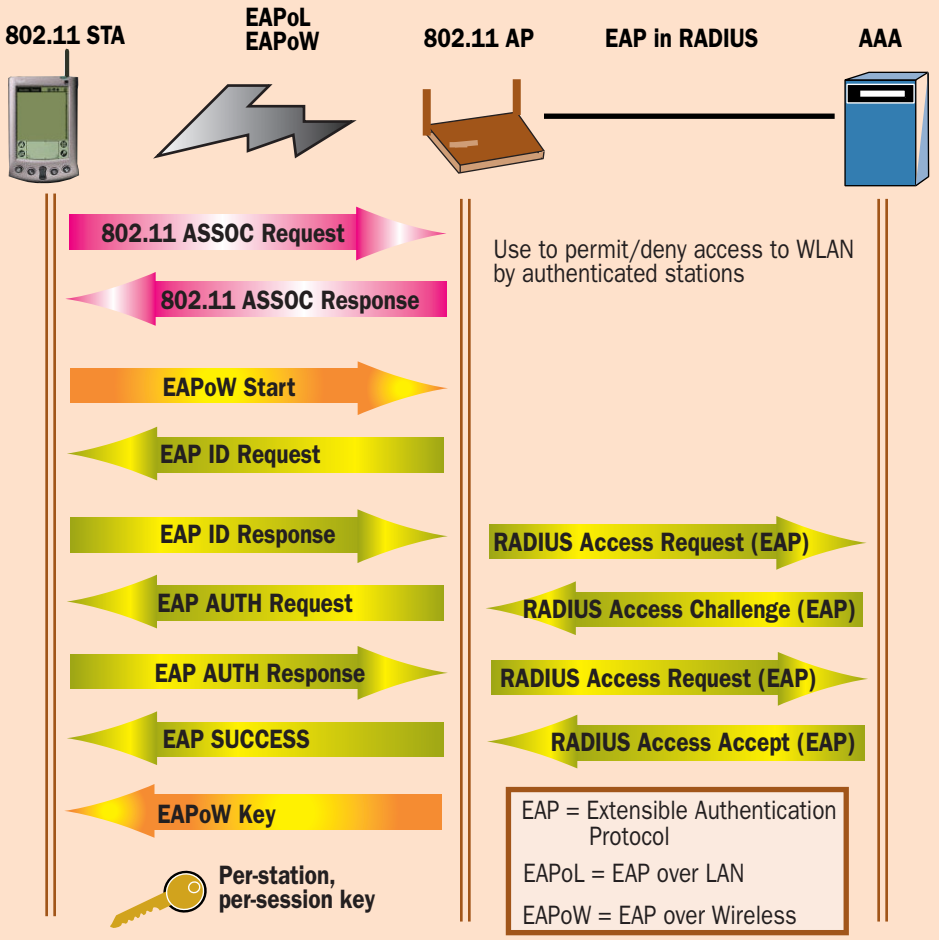
Most enterprises will adopt 802.1X—eventually

Authentication Risks

Access controls permit use by authorized stations while blocking others. As such, they depend upon our ability to identify and authenticate stations. WLANs pose some unique authentication risks, including:

■ **Lost or Stolen Cards:** Most wireless devices—PDAs, PC cards, compact flash—are small and portable. As a result, they are easily lost

FIGURE 2 802.1X Port Access Control



or stolen. When a card goes missing, MAC ACLs obviously must be updated. Shared keys may also require update if written to the card or stored without password protection on a lost PDA or laptop. Using 802.1X with credentials not stored on disk or ROM—for example, two-factor SecurID tokens—can reduce this risk.

■ **MAC Spoofing**: MAC ACLs are not foolproof, because some cards support configurable MAC addresses. An attacker can capture legitimate frames, extract a valid MAC address, and use it when the legitimate card goes offline. Combining MAC ACLs with some other type of authentication makes a WLAN less vulnerable to MAC address spoofing.

■ **Rogue Access Points:** Gartner estimates that one out of five companies has already been penetrated by unauthorized APs—i.e., those installed by enthusiasts within the company unwilling to wait for IT deployment. This statistic suggests that networks must be able to authenticate not only connecting stations, but APs themselves.

In some cases, the need for this kind of security clashes with the universal desire for ease of use. For example, Windows XP offers "wireless zero configuration," letting stations automatically connect to any discovered AP. This feature may be convenient, but many companies should disable the option, requiring that stations connect only to preferred APs.

At one out of five companies, employees may already have installed unauthorized access points

■ **Compromised Secrets:** Shared-key authentication is worthless once that key has been compromised. WLANs are especially vulnerable because WEP uses the same key for both authentication and encryption. Researchers have demonstrated that the WEP encryption standard does not prevent key cracking. By crunching captured frames with a program like WEPcrack, an attacker can learn the key(s) used to encrypt those frames in as little as 15 minutes.

802.1X reduces this risk by (1) using separate credentials for authentication and encryption, and (2) delivering per-station, per-session encryption keys that reduce the number of frames encrypted with the same key, making cracking harder and less valuable to attackers.

Confidentiality Concerns

Each company must determine its own requirement for data confidentiality. After the Best Buy incident, SecurityFocus participants debated whether credit-card numbers really require confidentiality. Public opinion aside, privacy legislation like the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley (GLB) Act and the U.K. Data Protection Act, require companies to keep non-public personal information private and secure. These mandates must be considered when deploying any kind of network, but the risk of disclosure is higher in a broadcast radio network.

When considering confidentiality, remember that operating a WLAN without encryption leaves it vulnerable to:

■ **Traffic Analysis:** Attackers can learn quite a bit from the headers surrounding even non-confidential payload. Valid SSIDs, MAC addresses and IP addresses can all be obtained by analyzing captured frames, helping an attacker penetrate wireless and adjacent networks. Destination addresses, DHCP requests, DNS queries and NetBIOS broadcasts can help attackers breach intranet servers and file shares. The less information you give away on the WLAN, the lower your risk.

■ **Disclosure of Private Data:** In my INT Media survey, privacy was the number-one security concern, important to 94 percent of those surveyed. Eavesdropping on wireless payload can disclose logins, passwords, file names, mail server addresses, database locations and more, depending upon the application. For example, capturing wireless inventory management traffic could reveal sales volumes, customer buying habits, and top-selling items. When assessing your own vulnerability to WLAN eavesdropping, consider visitors in your lobby and conference rooms, as well as neighboring offices above and below you. Careful antenna placement can reduce these vulnerabilities, but usually cannot eliminate them.

There are many options for providing WLAN payload confidentiality, some unique to wireless and others commonly used to provide secure remote access:

■ **WEP Encryption:** As previously noted, this weak link-level encryption is supported by most APs. Given enough traffic, a war driver can crack static WEP keys. However, WEP is still a good first step to eliminate casual eavesdropping, particularly in smaller WLANs where keys can be manually updated at regular intervals without difficulty.

■ **Proprietary Wireless Encryption:** Several vendors offer non-standard solutions for wireless authentication and confidentiality. For example, NetMotion protects data transmitted between a Mobility Server and Client with DES, 3DES,

Twofish or AES encryption, deriving unique session keys with Diffie-Hellman.

■ **Temporal Key Integrity Protocol:** TKIP is a standard now under development to mend the most glaring WEP weaknesses. TKIP is expected to use 802.1X for authentication and key delivery, and to encrypt with short-lived "temporal" keys that are refreshed often enough to prevent key reuse (the event that leads to WEP key cracking). If the IEEE approves TKIP this summer, firmware upgrades may be available for existing Wi-Fi products by the end of 2002.

■ **VPN Encryption:** WEP and TKIP encrypt frames on the wireless link only. PPTP, IPSec or L2TP-over-IPSec VPNs encrypt data all the way from remote access clients to security gateways at the private network edge. Wireless laptops and teleworker desktops already equipped with VPN clients for secure remote access over the Internet may reuse these clients to encrypt data over Wi-Fi. There are several alternatives for terminating the VPN tunnel:

■ **Tunnel to the AP:** A few access points can operate as VPN gateways, terminating PPTP or IPSec tunnels at the edge of the WLAN—for example, the Colubris CN1050.

■ **Tunnel to a VPN/Firewall:** Depending upon network size, traffic load and distribution, you may tunnel Wi-Fi to your existing VPN/firewall or deploy additional VPN/firewall(s).

■ **Tunnel to a WLAN Access Concentrator:** In larger WLANs where greater mobility and scalability are required, consider tunneling to a special-purpose wireless access appliance from Bluesocket, ReefEdge or Vernier Networks.

■ **Upper-Layer Encryption:** Methods commonly used to encrypt Internet applications can be used to protect wireless traffic, too. For example, mail messages over Wi-Fi can be encrypted with PGP or S/MIME. Remote administration can be protected with Secure Shell. Secure remote desktop access can be accomplished with a service like ExpertCity's GoToMyPC.

When choosing a solution, consider not only airlink encryption, but end-to-end network security. Those who want to wait before making a long-term investment in wireless security can leverage measures already deployed for Internet-based remote access. Doing so will improve near-term security and help you better understand the unique challenges associated with protecting WLANs.

Data Integrity And Reliability

Many companies take data integrity and reliability for granted, but risk-averse industries know better. These vulnerabilities exist in wired networks, but again are greater in WLANs:

■ **Replay:** According to INT Media survey results, wireless replay attacks are not very common—but they do happen. Unencrypted frames are easily captured and replayed. IPSec VPNs provide strong replay protection, but nothing prevents re-sending a captured frame that was encrypted with WEP. Ultimately, replay success depends on the application—for example, duplicate TCP data will usually be discarded.

■ **Forgery:** WEP includes a CRC that detects corruption, but cannot prevent a frame from being modified such that the CRC still passes. TKIP includes a stronger Message Integrity Code (MIC) to prevent forgery. In the meantime, if your business cannot risk data forgery or requires non-repudiation, use a VPN or higher-layer solution to ensure wireless data integrity.

■ **Spoofing:** In Ethernet LANs, IP spoofing of inside addresses can be blocked at the perimeter firewall. And ARP cache poisoning—a LAN attack that exploits the Address Resolution Protocol to redirect frames—cannot reach beyond the local subnet. These attacks are therefore primarily insider threats.

By contrast, on WLANs, outsider spoofing is much more likely. You can reduce this risk by using static ARP on the wired segment attached to your APs and avoiding unprotected DHCP—for example, bind IP addresses to known MAC addresses, or allow DHCP access only after 802.1X authentication.

■ **Session Hijacking:** Man-in-the-middle (MitM) attacks like session hijacking are possible in WLANs. An attacker can use a high-powered AP to intercept associate requests, masquerade as the legitimate AP, relay WLAN traffic to intended destinations, and return responses to requesting stations. Stations and intranet servers may be unaware that sessions have been hijacked. To reduce MitM risk, monitor for rogue APs and use 802.1X with strong mutual authentication. To limit what the MitM can do with intercepted traffic, use end-to-end encryption and data integrity.

■ **Packet Floods:** In recent years, on-line businesses have learned to protect Internet-facing servers from denial-of-service (DoS) attacks. Wireless APs and servers connected directly to the WLAN require similar protection. For example, if you place your APs on a firewall DMZ, use DoS thresholds to defeat TCP SYN or UDP packet floods generated by a war driver hoping to cripple your WLAN.

■ **Jamming:** WLANs are also vulnerable to low-tech jamming, where an attacker generates RF signal (noise) on the same channel(s) occupied by your WLAN. A WLAN analyzer can be used to locate the source. When jamming is unintentional—for example, a 2.4 GHz phone system or microwave—the offending signal source can often be moved. Alternatively, change the channel used by your AP or move to a different band (i.e., 802.11a).

Knowledge Is Power

According to Gartner research director John Pescatore, 30 percent of enterprises will suffer serious exposures by year end from deploying

It's estimated that 30 percent of enterprises will suffer serious exposure due to WLANs

Network security always requires up-front planning

WLANs without proper security. "Wireless LANs are broadcasting secrets of enterprises that have spent millions on Internet security," said Pescatore. "Because WLANs are on every executive's wish list, CIOs should [put] security measures in place now. Fixing the exposure after a hacking attack cannot recapture lost intellectual property and sensitive customer information."

But it is also important to keep this all in perspective. Every network technology has vulnerabilities. War driving and WEP flaws have simply heightened industry awareness of the risks inherent in wireless LANs. Secure network deployment always requires up-front planning to identify and address vulnerabilities in accordance with business risk.

After WLANs are deployed, continued vigilance is necessary. Perform regular site surveys to find unknown or misconfigured APs and stations. Conduct penetration tests (attempt to break into your own hardened stations, APs and wired network) to validate the security measures you have implemented. Use log monitoring and intrusion detection systems to spot unusual behavior originating from your WLAN. Knowledge is power—use it to keep your wireless LAN secure□

Companies Mentioned In This Article

Agere (www.agere.com)
AirMagnet (www.airmagnet.com)
Best Buy (www.bestbuy.com)
Bluesocket (www.bluesocket.com)
Cisco (www.cisco.com)
Colubris (www.colubris.com)
CVS (www.cvs.com)
Exodus (www.exodus.com)
ExpertCity (www.expertcity.com)
FedEx (www.fedex.com)
Funk (www.funk.com)
Hewlett Packard (www.hp.com)
Home Depot (www.homedepot.com)
INT Media Research (www.intmediaresearch.com)
Microsoft (www.microsoft.com)
NetMotion (www.netmotion.com)
Pasadena Networks (www.pasadena.net)
PepsiCo (www.pepsico.com)
Proxim (www.proxim.com)
ReefEdge (www.reefedge.com)
SecurityFocus (www.securityfocus.com)
Time Warner (www.aoltimewarner.com)
UPS (www.ups.com)
Vernier Networks (www.verniernetworks.com)