Wireless LANs provide mobility. Who does not want to be able to carry their laptop to the conference room down the hall and still have complete network access without worrying about network cables? Manufacturing companies are even using wireless LANs (WLANs) to monitor shop-floor machinery that is not traditionally accessible by network cabling. Increased mobility and accessibility improves communication, productivity, and efficiency. How much more productive could a team meeting be if all participants meeting in the conference room still had access to the network and the files relating to the project being discussed?

Wireless LANs can also provide a cost benefit. Installing and configuring wired communications can be costly, especially in those hard-to-reach areas. Ladders, drop ceilings, heavy furniture, knee pads, and a lot of time are often necessary to get all components installed and connected properly. By comparison, wireless LAN installations are a breeze. Plug in the access point, install a wireless NIC, and one is all set. An access point is the device that acts as a gateway for wireless devices. Through this gateway, wireless devices access the network. See Exhibit 1 for an illustration.

The increased mobility and cost effectiveness make wireless LANs a popular alternative. The Gartner Group has predicted that wireless LAN revenue will total $487 million in 2001, and the value of installed wireless LANs will grow to $35.8 billion by 2004. The Cahners In-Stat Group has predicted that the wireless LAN market will grow 25 percent annually over the next few years, from $771 million in 2000 to $2.2 billion in 2004. While these estimates are quite different, they share one

**PAYOFF IDEA**

Wireless LANs have several security issues that preclude them from being used for highly sensitive networks. Poor infrastructure design, unauthorized usage, eavesdropping, interception, DoS attacks, and client system theft are all areas one should analyze and consider. One can mitigate these risks by wrapping the communication in a VPN or developing one’s own creative solution, but this can be complicated. New advancements in wireless technology, along with changes in the WEP standard, may improve security as well as usability.
common theme: a significant number of new wireless LANs will be deployed and existing installations will be expanded. This growth will occur because increases in speed, decreases in price, and the adoption of a formal standard with broad industry support have all occurred in the past year.

STANDARDS

Before discussing security issues with wireless LANs, a discussion of the standards that are the basis for communication is in order. In June 1997, the IEEE (Institute of Electrical and Electronic Engineers) finalized the initial standard for wireless LANs, IEEE 802.11. This standard specifies a 2.4-GHz operating frequency with data rates of 1 and 2 Mbps and the ability to choose between using frequency hopping or direct sequence, two noncompatible forms of spread spectrum modulation. In late 1999, the IEEE published two supplements to the initial 802.11 standard: 802.11a and 802.11b.

Like the initial standard, 802.11b operates in the 2.4-GHz band, but data rates can be as high as 11 Mbps and only direct sequence modulation is specified. The 802.11a standard specifies operation in the 5-GHz band using OFDM (orthogonal frequency division multiplexing) with data rates up to 54 Mbps. Advantages of this standard include higher capacity and less RF interference with other types of devices. Although the
802.11a standard exists, there are currently no products on the market. They should start to become available in the fourth quarter of 2001.

Standards 802.11a and 802.11b operate in different frequencies; thus, there is little chance they will be interoperable. They can coexist on one network, however, because there is no signal overlap. Some vendors claim they will provide a dual-radio system with 802.11a and 802.11b in the future.

To complicate issues, Europe has developed the HiperLAN/2 standard, led by the European Telecommunications Standards Institute (ETSI). HiperLAN/2 and 802.11a share some similarities: both use OFDM technology to achieve their data rates in the 5-GHz range, but they are not interoperable.

For the remainder of this article, discussions will focus on 802.11b wireless LANs because they comprise the current installed base.

SECURITY ISSUES
Wireless LANs have major security issues. Default configurations, network architecture, encryption weaknesses, and physical security are all areas that cause problems for wireless LAN installations.

DEFAULT INSTALLATIONS
Default installations of most wireless networks allow any wireless NIC to access the network without any form of authentication. One can easily drive around with laptop in hand and pick up many network connections. Because this vulnerability is so prevalent, “war driving” is quickly replacing “war dialing” as the method of finding backdoors into a network. Wireless LAN administrators may realize that radio waves are easier to tap passively than cable, but they may not realize just how vulnerable they really are.

Wireless ISPs must be very conscious of their wireless network configurations. If someone is able to access their networks without authentication, they are essentially stealing service. The wireless ISP is losing revenue and the illegal user is taking up valuable bandwidth.

Once a user gains access to the wireless network, whether authorized or unauthorized, the only things preventing him from accessing unauthorized servers or applications are internal security controls. If these are weak or nonexistent, an unauthorized user could easily gain access to one’s network through the wireless LAN and then gain complete control of one’s network by exploiting internal weaknesses.

Denial-of-service attacks are also a very real threat to wireless networks. If running a mission-critical system on a wireless network, an attacker does not need to gain access to any system to cause damage and financial harm to an organization; they just need to flood the network with bogus radio transmissions.
MITIGATING RISK
To use wireless LANs in an enterprise or production environment, one must mitigate the inherent risk in current products and standards. Enterprise-level wireless LAN security focuses on two issues: network access must be limited to authorized users, and wireless traffic should be protected from sniffing. The 802.11b standard does include some security mechanisms, but their scalability is questionable.

MAC ADDRESS
One way to secure access to a wireless network is to instruct access points to pass only those packets originating from a list of known addresses. Of course, MAC (Media Access Control) addresses can be spoofed, but an attacker would have to learn the address of an authorized user's Ethernet card before this is successful. Unfortunately, many wireless cards have the MAC address printed right on the face of the card.

Even if the user and administrator can secure the card address, they still have to compile, maintain, and distribute a list of valid MAC addresses to each access point. This method of security is not feasible in a lot of public WLAN applications, such as those found in airports, hotels, and conferences, because they do not know their user community in advance. Additionally, each brand of access point has some limit on the number of addresses allowed.

SERVICE SET ID
Another setting on the access point that can be used to restrict access is the network name, also known as the SSID (Service Set ID). An access point can be configured to allow any client to connect to it or to require that a client specifically request the access point by name. Although this was not meant primarily as a security feature, setting the access point to require the SSID can let the ID act as a shared group password.

As with any password scheme, however, the more people who know the password, the higher the probability that an unauthorized user will misuse it. The SSID can be changed periodically, but each user must be notified of the new ID and reconfigure their wireless NIC.

WIRED EQUIVALENT PRIVACY (WEP)
The 802.11b standard provides encrypted communication between clients and access points via WEP (Wired Equivalent Privacy). Under WEP, users of a given access point often share the same encryption key. To achieve mobility within a campus, all access points must be set to use the same key and all clients have the same encryption key as well. Additionally, data headers remain unencrypted so that anyone can see the source and destination of data transmission.
WEP is a weak protocol that uses 40- and 128-bit RC4. It was designed to be computationally efficient, self-synchronizing, and exportable. These are the characteristics that ultimately crippled it. The following are just a few of the attacks that could easily be launched against WEP:

- Passive attacks to decrypt traffic based on statistical analysis
- Active attacks to inject new traffic from unauthorized mobile stations, based on known plaintext
- Dictionary-building attack that, after analysis of about a day’s worth of traffic, allows real-time automated decryption of all traffic

With these limitations, some vendors do not implement WEP, although most provide models with and without it. An access point can be configured to never use WEP or to always require the use of WEP. In the latter case, an encrypted challenge is sent to the client. If the client cannot respond correctly, it will not be allowed to use the access point, making the WEP key another password. As with using the SSID as a password, the administrator could routinely change the WEP key, but would have the same client notification and configuration issues.

Of course, an attacker possessing the WEP key could sniff packets off the airwaves and decrypt them. Nonetheless, requiring WEP substantially raises the minimum skill set needed to intercept and read wireless data.

**AUTHENTICATION SOLUTIONS**

Some vendors offer proprietary solutions to the authentication/scalability problem. The wireless client requests authorization from the access point, which forwards the request to a RADIUS server. Upon authorization, the RADIUS server sends a unique encryption key for the current session to the access point, which transmits it to the client. While this standard offers a solution to the shared key problem, it currently requires an organization to buy all the equipment from one vendor. Other vendors use public key cryptography to generate per-session keys.

This authentication solution resembles pre-standard implementations of the pending IEEE 802.1x standard that will eventually solve this problem in a vendor-interoperable manner. The 802.1x standard is being developed as a general-purpose access-control mechanism for the entire range of 802 technologies. The authentication mechanism is based on the Extensible Authentication Protocol (EAP) in RADIUS. EAP lets a client negotiate authentication protocols with the authentication server. Additionally, the 802.1x standard allows encryption keys for the connection to be exchanged. This standard could appear in wireless products as early as 2002.

While waiting for 802.1x, there are a few other approaches the administrator can take to increase the security of a wireless LAN.
THIRD-PARTY PRODUCTS
Several products exist to secure wireless LANs. For example, WRQ's Net-Motion (www.netmotionwireless.com) requires a user login that is authenticated through Windows NT. It uses better encryption (3DES and Twofish) than WEP and offers management features such as the ability to remotely disable a wireless network card's connection. One of the main issues with this solution is that the server currently must run on Windows NT and client support is only provided for Windows 95, 98, ME, and CE. Support for Windows 2000 server and client is currently under development.

GATEWAY CONTROL
Gateway solutions create special sub-nets for wireless traffic. Instead of using normal routers, these sub-nets have gateways that require authentication before packets can be routed. The sub-nets can be created with VLAN technology using the IEEE 802.1Q standard. With this standard, administrators can combine selected ports from different switches into a single sub-net. This is possible even if the switches are geographically separated as long as VLAN trunking is supported on the intervening switches. Nodes that use VLAN ports cannot access addresses on other sub-nets without going through a router or gateway, even if those other sub-nets are located on the same physical switch as the VLAN ports.

Once the VLAN is established, administrators need to create a gateway that will pass traffic only from authorized users. A VPN gateway can be used because the function of a VPN server is to require endpoint. Using a VPN server as the gateway not only requires authentication of the tunnel endpoint, but it also encrypts the wireless stream with a key unique to the tunnel, eliminating the need to use the shared key of WEP.

The VPN approach is hardly ideal, however. Understanding VPN technology, selecting a VPN gateway, configuring the server, and supporting clients are complex tasks that are not easy for the average LAN administrator to accomplish.

Another solution, currently used by Georgia Tech, uses a special firewall gateway. This approach still uses the VLAN approach to aggregate wireless traffic to one gateway; but instead of being a VPN, this gateway is a dual-homed UNIX server running specialized code. The IT staff at Georgia Tech uses the IP Tables firewall function in the latest Linux kernel to provide packet filtering. When a system joins the wireless network, the firewall/router gives it a DHCP address. To authorize access, the client must open a Web browser. The HTTP request from the client triggers an automatic redirect authentication page from the gateway and the authentication request is passed to a Kerberos server. If authentication is successful, a Perl script adds the IP address to the rules file, making it a "known" address to the IP Tables firewall process.
From the user’s perspective, they must launch a browser and enter a userid and password to gain access to the network. No client installation or configuration is required. Of course, this method only provides authentication — not encryption — and will not scale over a few hundred simultaneous users. This solution is unique and elegant because it allows complete on-the-fly network access without making any changes to the client, and it supports network cards from multiple vendors. This configuration is very useful in public WLAN applications (airports, hotels, conferences, etc.).

**CONCLUSION**

Wireless LANs have several security issues that preclude them from being used for highly sensitive networks. Poor infrastructure design, unauthorized usage, eavesdropping, interception, DoS attacks, and client system theft are all areas that one needs to analyze and consider. One can mitigate these risks by wrapping the communication in a VPN or developing one’s own creative solution, but this can be complicated. New advancements in wireless technology, along with changes in the WEP standard, may improve security as well as usability.

Manday Andress, CISSP, is founder and president of ArcSec Technologies. A frequent speaker and author, she is a veteran of Exxon USA, Deloitte & Touche, and Ernst & Young.