Wireless LAN technology is a swiftly moving target. Knowing the basics can help you deploy it safely in your organization.

Gilbert Held

The ABCs of IEEE 802.11

During summer 2001, it was relatively easy to pick up a newspaper or trade magazine and find comments concerning wireless local area networks (WLANs) and the security problems they presented. Unfortunately, in a way similar to the improper use of baud and bit per second, some authors seem to have misunderstood the technology they were writing about, providing readers with a limited indication of the severity of security-related problems. Like Don Quixote, let me attempt to right a wrong by first asking you to recognize that WLAN is a series of standards and not just one standard.

WHEN ONE IS NOT ENOUGH

WLANs have been around for several years and do not actually represent a recent phenomenon. Such LANs operate in the unlicensed Industrial, Scientific, and Medical (ISM) frequency spectrum—a frequency band (or, more correctly, several frequency bands) that different products can use as long as they comply with certain regulatory rules. These rules cover characteristics such as radiated power and the manner in which modulation occurs. Although many regulatory authorities have the same rules, there are differences in power and modulation methods used by WLANs in the ISM band that preclude worldwide compatibility.

Operating frequencies

Until a few years ago, most WLANs operated in the 900-MHz ISM band; the actual frequency reserved by the FCC is 902 to 928 MHz. The other two ISM bands include the 2.4-GHz band (which really ranges from 2.4 to 2.4853 GHz) and the 5.7 GHz band (from 5.725 to 5.85 GHz). The latter is also referred to as the National Industrial Infrastructure (NII) band. Because the use of ISM bands does not require an FCC license, these bands are popular for WLANs and devices as diverse as portable phones and microwave ovens.

Transmission methods

The initial IEEE 802.11 standard supported three transmission methods—infrared, direct-sequence spread spectrum (DSSS), and frequency-hopping spread spectrum (FHSS)—although a single product would use only one method. All three transmission methods can operate at 1 and 2 Mbps.

Because infrared transmission operates in the light spectrum, it does not require a license from the FCC and was used years ago in wireless devices that were not 802.11 compatible.

Both DSSS and FHSS represent transmission techniques "borrowed" from military development. The military originally used such techniques to overcome the effects of radio jamming and potential enemy eavesdropping. Spread-spectrum transmission expands or spreads a signal such that it appears to represent random background noise instead of a data transmission signal.

DSSS uses a spreading code to replicate each data bit; it produces n transmission bits for each data bit. Typically, n is an odd number, which lets a receiver examine the composition of each of the spread bits and select the value that is in the majority. That is, if the transmission uses a spreading code with $n = 11$, and six bits are set to 0 and

1520-9202/01/$10.00 © 2001 IEEE

five bits are set to 1, the receiver will assume that the bit's correct value is 0. FHSS, the second spread spectrum method supported by IEEE 802.11, transmits each bit at a different frequency.

Unlike military spread-spectrum systems—in which the spreading code or frequency-hopping pattern is secret—DSSS and FHSS use a code or pattern that is well known when used by WLANs. Such public disclosure is necessary because the code or pattern is a governing factor for equipment interoperability.

Alphabet soup of standards

IEEE published the initial standard in May 1997. During 1999, it also published an appendix, now referred to as IEEE 802.11b. IEEE 802.11b specifies that devices modulate data using DSSS at data rates of 1, 5.5, and 11 Mbps. The actual data rate employed depends on the distance between devices, which in turn governs signal quality and strength. In general, the closer two devices are to one another, the higher the obtainable transmission rate. Although several manufacturers produced IEEE-802.11-compatible products early on, significant interest in WLANs did not arise until after IEEE 802.11b devices reached the market.

As you might expect in a wireless environment, security can be an important issue.

In 1999, IEEE approved a third wireless-LAN standard, now referred to as IEEE 802.11a. Designed to support data rates as high as 54 Mbps, this standard required a new approach to counter the problem of delay spread in the 2.4-GHz frequency band. Delay spread results from the echoing of a transmitted signal off objects such as walls, furniture, and floors. These echoes result in a series of signals reaching the receiving antenna at different points in time because the echoes traverse different paths. Thus, another name for this type of delay is *multipath* delay.

At the receiver, it is important to unravel the divergent radio frequency signals. Doing so requires a special processor called a *base band processor* or *equalizer*. To unravel the signal, the delay spread must be less than the symbol or baud rate (the rate at which the sender transmits the smallest individual pieces of information). Otherwise, a portion of the delayed signal will spread into the next symbol's transmission. This delay spread in effect places a cap of between 10 and 20 Mbps on the maximum obtainable bit rate.

Bypassing the problem associated with the previously mentioned delay spread caused the standard to incorporate a different modulation method, *coded-orthogonal frequency-division multiplexing*. Under COFDM, devices transmit data in parallel using a series of relatively low-speed subcarriers. This action slows the symbol rate so that it is much less than the delay spread. Because achieving a high data transmission rate requires a relatively large number of subcarriers, its developers designed IEEE 802.11a to operate in the 5-GHz band.

Although a few vendors could have shipped 802.11a products by the time you read this article, for the foreseeable future, expect the vast majority of wireless-LAN products to be IEEE 802.11b compatible.

ATTENUATION

A funny thing happened on the road to IEEE 802.11a: It had to recognize a law of physics, namely, higher frequencies attenuate—become weaker as they get further from their source—more rapidly than lower frequencies. Because regulations limit a WLAN's radiated power, the 5-GHz frequency will force organizations to use multiple access points, whereas under IEEE 802.11b a single 2.4-GHz band access point could suffice. Thus, the potential increase in data rate (to 54 Mbps) offered by IEEE 802.11a is offset by a decrease in the radius of transmission from an access point to a client.

Perhaps recognizing the range limitation, members of the IEEE 802.11 task force are sharpening their pencils and drafting the 802.11g standard. This standard essentially enhances 802.11b by supporting 20 Mbps operation in the 2.4 GHz band and providing backward compatibility with 802.11b.

In an interesting side note, at the time I was writing this article, the IEEE was considering a proposal by wireless chipmaker Intersil. This company's dual-band chip set would support 2.4- and 5-GHz operations, in effect supporting both 802.11a and 802.11g standards. Although not currently specified, another letter of the alphabet will probably arise to extend the 802.11 moniker, this time to indicate dual-band operation.

SECURITY

As you might expect in a wireless environment, security can be an important issue. If you read one of several articles appearing in *The New York Times* or *The Wall Street Journal*, you learned that it was a relatively easy process for two guys in a van to drive from one Silicon Valley parking lot to another and eavesdrop on wireless LAN transmissions in different buildings. These articles appeared at approximately the same time as a technical paper on intercepting mobile communications from the University of California, Berkeley (Nikita Borisov, Ian Goldberg, and David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *Proc. 7th Ann. Int'l Conf. Mobile Computing and Networking (Mobicom)*, 2001; http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf). Because of this coincidence, many people formed the false impression that the flaws in 802.11 security identified by the UC Berkeley troika were related to the ease of reading wireless-LAN

activity. In actuality, these problems stem from two separate but related issues, so let's discuss security in an 802.11 environment.

WEP

Presently, the Wired Equivalency Privacy (WEP) algorithm, part of the 802.11 standard, provides security for wireless transmission. WEP uses the RC4 encryption algorithm, a stream cipher. A stream cipher is a mathematical algorithm that expands a short key into an infinite pseudorandom key stream.

WEP uses a 10-digit hexadecimal character key to create a 40-bit key to which a 24-bit initialization vector (IV) is added. A transmitting station will apply an XOR (exclusive OR) to the key stream with the plaintext to generate ciphertext (encrypted text). A receiver configured with the same 10-hex character key can XOR the key stream with the received ciphertext to generate the original message's plaintext.

To avoid encrypting two frames with the same key stream, the IV augments the shared secret key to produce a different RC4 key for each packet. Because WEP uses a 24-bit IV, which a transmitter sends in the plaintext portion of a message, a busy access point will exhaust its use of IVs within a quarter of a day or less. So in a short time period, a hacker could record two ciphertext messages that the sender encrypted with the same key. The hacker could then possibly recover the plaintext using statistical analysis.

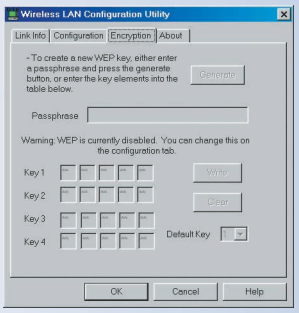
A second limitation of WEP is the fact that all participants must have the same key. This means that public portals—such as those found in hotels, airport waiting rooms, and coffee shops—provide no security, because each person uses the same key. So aside from constant monitoring, there is nothing to stop a hacker from using a WLAN monitor to record the activity of legitimate users. In fact, one of the more popular wireless monitors, Airopeek, a program from WildPackets, includes the capability to enter the WEP key to provide the operator with plaintext decodes. Although their developers intended Airopeek and similar programs to facilitate problem resolution, these programs can also record everything flowing though the air.

The UC Berkeley paper also noted additional flaws in the WEP algorithm that apparently caught the attention of equipment vendors and the IEEE, because each took steps to fix these flaws. For example, several vendors announced proprietary security solutions, some of which involve using an authentication server that only lets predefined users access the network. Other vendors have attacked WEP's limitations. Some vendors support the use of a longer 128-bit key, while others added proprietary encryption, which in effect locks users into a particular vendor.

User authentication

In addition, the IEEE is working on the evolving 802.1x standard, which defines how users authenticate themselves to a network. Based on the Internet Engineering Task Force's RFC 2284, 802.1x specifies how to encapsulate the extensible authentication protocol (EAP)—an RFC-2284-defined, general-purpose protocol for authentication—into a LAN frame.

Figure 1. The SMC Networks EZ Wireless PC card, like many other vendor products, disables WEP by default.



WHAT YOU CAN DO

While waiting for the dust to settle over different wireless security methods, you can do several things to secure your wireless network.

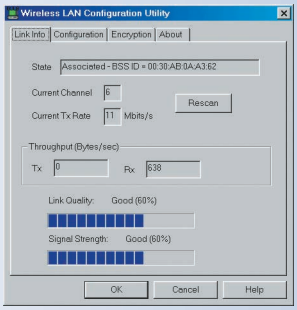
Enable WEP

I have worked with 802.11 hardware from over a dozen vendors. Perhaps one item all vendor equipment has in common is that by default, WEP is disabled. It was for this very reason that the two guys in a van could so easily read so much traffic. Thus, if you pull an access point and a few client cards out of a box to establish a WLAN, you are literally operating naked. Figure 1, which shows the default setting for an SMC Networks EZ Wireless PC card, underscores this point. By configuring your access point and wireless clients to use WEP, you at least make it a bit more difficult for unauthorized people to read your traffic. Enabling WEP will, at a minimum, preclude real-time decodes by unauthorized persons.

Position your access point

The conventional wisdom for setting up an access point is to position the device such that it provides an optimum level of signal strength to all areas where wireless clients can reside. Unfortunately, conventional wisdom does not consider RF (radio frequency) leakage outside the building and into the parking lot, where unauthorized people can retrieve the signals. To minimize this potential RF leakage, you can use a notebook computer with a wireless client and observe the access point's link quality and sig-

Figure 2. Most products provide a screen that displays link quality and signal strength. Use this display to assist in positioning an access point to minimize RF leakage.



nal strength as you move about your organization. Figure 2 illustrates the Link Info tab on the utility program provided by SMC Networks with its client network cards. By walking the interior and exterior of your organization's building and using a cell phone to ask another employee to move the access point, you can probably minimize the RF leakage.

Minimize bridging

In effect, an access point represents a data-link-layer bridge. As the access point develops its port address table, it will initially broadcast all the frames received on the connected hub, including frames initiated by employees working at hardwired systems. These frames, however, can contain logon data and other sensitive information that is typically unencrypted and hence vulnerable to hackers.

To minimize the bridging effect, you can consider connecting access points to your network at the network layer. To do so you must use a router or layer-3 switch that will route IP transmissions to the access point for distribution to wireless stations.

Although the only secure wireless network is probably one located in a lead-lined vault, you can do several things to limit an organization's vulnerability. Each of the items mentioned here can add another degree of protection to your organization's WLAN. ■

Gilbert Held *is a lecturer, author, and consultant specializing in data and computer communications. He is the author of* Deploying Wireless LANs *(McGraw-Hill, 2001) and* Voice & Data Internetworking, 3rd edition *(McGraw-Hill, 2001). Contact him at gil_held@yahoo.com.*

For further information on this or any other computing topic, visit our Digital Library at http://computer.org/publications/dlib.