The IEEE 802.11b Security Problem, Part 1

Joseph Williams

Be aware of the security issues a wireless LAN can pose, and take steps to use its built-in security features.

Functionally, there is no inherent security for IEEE 802.11b. In early April 2001, Peter Shipley and Matt Peterson illustrated several serious security holes in 802.11b networks. They did so in a single day by eavesdropping on more than 80 corporate wireless networks that implemented virtually no security. The duo demonstrated that anyone sitting in a parking lot with $150 worth of technology could pick up information from these wireless networks (Kevin Poulsen, "War Driving by the Bay," *The Register*, 20 Apr. 2001, http://www.theregister.co.uk/content/8/18285.html).

Concurrently and independently, researchers at the University of California, Berkeley, discovered serious flaws in the only built-in security technology for 802.11b, the Wired Equivalent Privacy (WEP) algorithm ("Security of the WEP Algorithm," http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html).

How important are these problems? Understood in the appropriate context and regardless of the raging debates surrounding WEP, they have serious implications for the security architecture of 802.11b networks.

WHAT IS 802.11B?

IEEE 802.11b is a standard for wireless local area networks (WLANs). It covers systems in which an omnidirectional wireless radio generates a nominal 2.4-GHz carrier wave that communicates over a theoretical range of 1,000 feet (and a practical limitation of less than 350 feet) with devices—typically laptops—equipped with 802. 11b transceivers. Directional radios have a much higher range (up to 30 miles) but are limited to line of sight. Although directional radios are used in *fixed wireless* networks, I do not specifically discuss such networks here.

Most systems encode 802.11b data using direct-sequence spread-spectrum technology. DSSS works by taking a data stream of 0s and 1s and modulating it with a second pattern based on complementary code keying. This method then modulates the CCK code word with quadrature-phase shift-keying (QPSK) technology to yield 22 MHz of frequency spectrum.

The 802.11b specification targets a theoretical throughput of 11 Mbps—more than seven times a traditional T1 connection. A series of wireless radios (called *Access Points*) deployed throughout an installation provides campus-wide connectivity. These Access Points thus provide blanket coverage for mobile workers as they move from park benches to conference rooms to drop-in offices. The WLAN industry has not established an exact vocabulary, but the device that communicates with the wireless radio Access Point is usually called the *station*.

In an 802.11b Basic Service Set (BSS), the Access Point acts as a bridge for a set of associated stations—PCs, laptops, handheld devices, and 802.11b-enabled IP (Internet protocol) phones—outfitted with wireless network interface cards (NICs). Most Access Points act as a MAC (media access control) level bridge, letting the WLAN serve as a natural extension of a wired network. Thus, Access Points act as a bridge between wireless and wired LANs. They give mobile workers complete connectivity to the corporate LAN and to the Internet.

Continued on page 91

1520-9202/01/$10.00 © 2001 IEEE

Continued from page 96

Organizations have extensively deployed 802.11b networks on campus-sized environments as well as in the home, seeking the advantages discussed in the "WLAN Benefits" sidebar. In addition, companies have deployed several 802.11b networks in public-space domains—airport lounges, coffee shops, shopping malls, and hotels—to keep mobile employees connected away from the office. Several ventures have implemented value-added services through 802.11b wireless portals, such as a boarding call sent to your computer to tell you when a flight is ready.

The Wireless Ethernet Compatibility Alliance is pushing a version of 802.11b called Wi-Fi. WECA's mission is to certify interoperability of Wi-Fi products and to promote Wi-Fi as the global WLAN standard across all market segments. Two of the more active Wi-Fi vendors have been MobileStar Network—which scored a major win in January 2001 by signing a deal with Starbucks—and Wayport, which focuses more on business travelers by providing public Wi-Fi at airports and hotels.

WLAN Benefits

With WLANs (wireless local area networks), users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. WLANs offer the following productivity, service, convenience, and cost advantages over traditional wired networks, according to the Wireless LAN Association (http://www.wlana.org/learn/educate2.htm#benef):

- ***Mobility.*** **WLAN systems can provide LAN users with access to real-time information anywhere in an organization. This mobility supports productivity and service opportunities not possible with wired networks.**
- ***Installation speed and simplicity.*** **Installing a WLAN system can be fast and easy, and can also eliminate the need to pull cable through walls and ceilings.**
- ***Installation flexibility.*** **Wireless technology lets the network go where wire cannot go.**
- ***Reduced cost of ownership.*** **Although the initial investment required for WLAN hardware can be higher than the cost of wired-LAN hardware, overall installation expenses and life cycle costs can be significantly lower. A WLAN's long-term cost benefits are greatest in dynamic environments that require frequent network moves, additions, and changes.**
- ***Scalability.*** **Network administrators can configure WLAN systems in various topologies to meet the needs of specific applications and installations. These easily changed configurations range from peer-to-peer networks—suitable for a few users—to full-infrastructure networks with thousands of users. These large networks allow roaming over a broad area.**

BUILT-IN 802.11B SECURITY MEASURES

Anyone within range of the Access Point radio can potentially eavesdrop on WLAN traffic or use the Access Point to access any connected network. In fact, unauthorized joyriders surf countless corporate networks and the Internet through unprotected Access Points; this is the point Shipley and Peterson were making with their demonstration. This isn't to say that 802.11b networking is inherently without any built-in security features.

At the simplest level, 802.11b enables two types of security: encryption (to preclude eavesdropping) and authentication (to prevent unauthorized users from accessing the network). When Shipley and Peterson were driving around Silicon Valley discovering unsecured WLANs, they also discovered failures of both types of security. Indeed, manufacturers typically ship 802.11b products with all the security features disabled by default, so Shipley and Peterson's findings were certainly not a surprise.

To associate with each other, Access Points and stations exchange various types of management frames, which are used to help determine who is allowed to join the network. For example, Access Points can periodically transmit beacon frames containing a unique identifier, known as a service set identifier (SSID), for the Basic Service Set. Stations use an SSID to gain access to a network, as described later.

Stations also transmit probe frames to discover Access Points. When a station finds an Access Point, it initiates an association and proposes an authentication method. The default association method, Open System Authentication, actually provides no authentication at all. In Open System Authentication, any station can join the BSS (Lisa Phifer, "Wireless Privacy: An Oxymoron?" http://www.80211-planet.com/columns/article/0,4000,1781_786641,00.html). The station can associate with any Access Point and "listen" to all data sent as plaintext. Network administrators usually implement this type of association when ease-of-use is the main issue or they're not concerned with security.

It has been widely suggested that frequency-hopping WLAN systems (802.11b uses a spread-spectrum technology) would be less vulnerable to security attacks than other WLANs. This is not true; in frequency-hopping systems, Access Points transmit the hopping codes and timings in plaintext, which is easily available to an attacker ("WLAN Response of WEP Security," http://slashdot.org/articles/01/02/15/1745204.shtml).

SSID

Administrators can implement network access control using an SSID associated with an Access Point or with a group of Access Points. The SSID provides a mechanism to segment a wireless network into multiple networks serviced by one or more Access Points. Each Access Point's programming includes an SSID corresponding to a specific wireless network. The SSID is a unique string that identifies the network, but it is the same string for all users on the network. To access this network, a client computer's configuration must include the correct SSID. A building might be segmented into multiple networks by floor or department. Typically, a client computer can use multiple SSIDs for users who require access to the network from various locations.

Because a client computer must present the correct SSID to access the Access Point, the SSID acts as a simple password and consequently provides some measure of security. However, this minimal security is compromised if, as is common, the administrator configures the Access Point to broadcast its SSID (Asma Yasmin, "Known Vulnerabilities in Wireless LAN Security," 10 Nov. 1999, http://www.tml.hut.fi/Studies/Tik-110. 300/1999/Wireless/vulnerability_4.html). With this broadcast feature enabled on a wireless network, any client computer not configured with a specific SSID can receive the SSID and gain entry to the Access Point.

Thus, the SSID actually provides virtually no security benefits at all—hackers can easily sniff it in plaintext from every packet (Carole Fennelly, "Let Security Hound You," *IBM developerWorks*, May 2001 http://www-106.ibm.com/developerworks/library/wi-sec.html). So the SSID's primary value is to partition traffic to a particular network.

MAC address filtering

Although an Access Point has an SSID for identification, a station uses the unique MAC address of its 802.11 network card as an identifier. To increase an 802.11 network's security, you can program each Access Point with a list of MAC addresses associated with the client computers allowed to communicate through the Access Point. If a client's MAC address is not on this list, the network does not let the client associate with the Access Point.

MAC address filtering provides stronger security than relying on SSIDs, but it comes with somewhat cumbersome administrative overhead: Administrators must manually program each Access Point with a list of MAC addresses and keep the list current. The administrative overhead of provisioning individual Access Points—there is no open-standard method of sharing access lists among Access Points—limits this approach's scalability. Thus MAC address filtering is best suited for small networks.

A determined hacker could identify and counterfeit the valid MAC addresses used on the network cards. After capturing an authorized MAC address, an intruder could easily program her own network card to have the same MAC address and gain access to the WLAN.

Wired Equivalent Privacy (WEP)

Network administrators can secure WLANs by employing techniques specified in the Wired Equivalent Privacy (WEP) standard. Its developers designed WEP so that 802.11 networks would have confidentiality similar to that of standard LANs. WEP uses an algorithm-based encoding system to protect wireless communication from eavesdropping. Most WEP implementations also authenticate stations seeking to join a BSS, thereby preventing unauthorized access to the WLAN.

In other words, when enabled, WEP encrypts the data portion of each packet exchanged between the station and the Access Point. It uses either a 40- or 128-bit encryption algorithm and relies on a secret key that the station and Access Point share. The station and Access Point use the secret key to encrypt packets before transmitting them. The receiver also uses an integrity check to ensure that packets remain unmodified in transit. The WEP standard does not specify how to establish the shared key. In practice, most implementations have all stations and Access Points share a single key.

In addition, some implementations use WEP in conjunction with the optional shared-key authentication algorithm to prevent unauthorized devices from associating with an 802.11b network. If the station proposes shared-key authentication, the Access Point generates a random 128-bit challenge. The station returns the challenge, encrypted with a shared key—a secret configured into both the station and the Access Point. The Access Point decrypts the challenge using a CRC (cyclic redundancy checker) to verify its integrity. If the decrypted frame matches the original challenge, the Access Point considers the station authentic. The Access Point and station repeat the challenge/response handshake in the opposite direction for mutual authentication.

It is perfectly reasonable to enable both the encryption and authentication features of WEP. Unfortunately, WEP uses the same shared key for encrypting/decrypting data frames and for authenticating the station. It is a major risk to have both encryption and authentication keys be the same.

WEP security is also not available in ad hoc (or peer to peer) 802.11b networks that do not use Access Points.

These networks would include, for example, a room full of laptop users who create a peering network using 802.11b. In this situation, the laptops connect to each other via their station transmitters but do not use an Access Point radio. The only security enabled on such a network would be whatever the laptop operating systems' provided, which is usually minimal.

Impact of WEP on WLAN performance

WLAN performance metrics are still highly debated and you should take them with a grain of salt until the technology is more mature. However, a few ad hoc studies are measuring whether WEP significantly affects WLAN performance. The results are somewhat contradictory, but one of the more credible sources reported minimal degradation of WLAN performance for either 40- or 128-bit WEP, as Table 1 shows (Rob Flickenger, "Performance Test: 802.11b Takes a Lickin' and Keeps on Tickin'," *O'Reilly Network*, 29 Mar. 2001, http://www.oreillynet.com/pub/a/wireless/2001/03/29/microwave.html).

Other sources suggest WEP degrades throughput by as much as 16 percent, although much of the degradation may be due more to the product architecture than to WEP itself (Andrew Garcia, "Performance Tests," *ZDNet Reviews*, 15 Feb. 2001, http://www.zdnet.com/products/stories/reviews/0,4161,2686384,00.html).

Table 1. Impact of WEP on WLAN performance.

	Actual throughput (bps)*		
Nominal throughput (Mbps)	No WEP	40-bit WEP	128-bit WEP
1	1,048,576	1,175,773	1,178,175
2	2,128,106	2,120,282	2,116,391
5.5	3,673,355	3,627,149	3,650,106
11	4,164,020	3,857,637	3,806,711

* Performance at 25 feet, through three walls and a solid wood door.

Short answer to WLAN security

Enabling all of the 802.11b security features collectively—SSID, MAC address filtering, and WEP—provides the most secure environment for WLAN traffic without having to resort to external measures. Figure 1 shows where these different features fit in such a network.

It is important to remember that physical security usually doesn't prevent intruders from getting close to a WLAN, so you must proceed on the assumption that intruders can and will snoop WLAN traffic. If you implement only built-in 802.11b security measures, be prepared to accept the likelihood that a determined hacker will defeat the 802.11b security and use a WLAN Access Point to reach the corporate network.

So, 802.11b security measures will be a sufficiently effective deterrent for some casual networking environments. As with any networking environment, a competent security analysis is critical when deploying WLANs. However, it is highly unlikely that most enterprise computing environments will find the inherent 802.11b security measures sufficient.

A growing consensus among industry experts charges that corporate users are not using WEP at all or, if they are, they are doing an inadequate job of addressing overall security management ("802.11b Security Flaws Being Addressed," *MobileInfo.com*, May 2001, http://www.mobileinfo.com/News_2001/Issue20/WLAN_Security.htm). WEP, SSID, and MAC address filtering—even if inadequate against a determined hacker—are better than no security at all. At a minimum, these methods will collectively thwart the opportunistic or accidental hacker.

SECURITY ISSUES

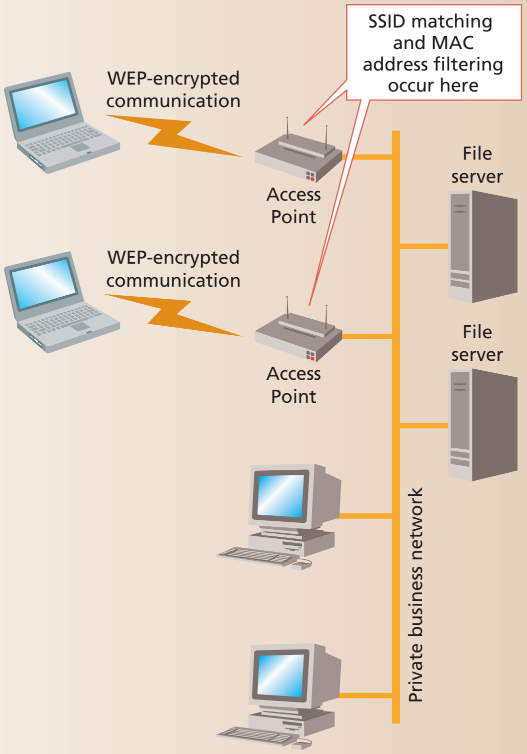
IEEE 802.11b-related security issues range from security management to inherent weaknesses of the underlying technologies. In addition, WLANs are subject to the same attacks that target traditional LANs.

High degree of management for WEP

When coupled with SSID and MAC address filtering, WEP security is best suited for small, tightly managed networks. For large networks, the administrative burden of maintaining WEP encryption keys on each client system and each Access Point, and maintaining a current list of valid MAC addresses on each Access Point make the WEP solution impractical. In addition, because all clients and Access Points use the same WEP encryption key, a lost or stolen client system requires an administrator to change all keys.

The point at which the number of wireless client systems becomes unmanageable varies, depending on the organization's ability to administer the network, its choice of security methods (SSID, MAC address filtering, WEP, or all three), and its tolerance for risk. If a company uses MAC address filtering on its wireless network, the maximum number of MAC addresses that each of the installation's Access Points can handle fixes the maximum number of client systems. In some cases, this upper limit is 255. However, the manageable number of clients under MAC address filtering will likely be considerably less than 255 for most organizations.

Figure 1. Using SSIDs, MAC address filtering, and WEP-based encryption protects wireless networks.


SSID matching and MAC address filtering occur here
WEP-encrypted communication
Access Point
File server
WEP-encrypted communication
Access Point
File server
Private business network

Circulation: IT Professional (ISSN 1520-9202) is published bimonthly by the IEEE Computer Society. IEEE Headquarters, Three Park Avenue, 17th Floor, New York, NY 10016-5997; IEEE Computer Society Publications Office, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; voice +714 821 8380; fax +714 821 4010; IEEE Computer Society Headquarters, 1730 Massachusetts Ave. NW, Washington, DC 20036-1903. Annual subscription: $36 in addition to any IEEE Computer Society dues. Nonmember rates are available on request. Back issues: $10 for members, $20 for nonmembers. This magazine is also available on microfiche.

Postmaster: Send address changes and undelivered copies to IT Professional, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855. Periodicals Postage Paid at New York, N.Y., and at additional mailing offices. Canadian GST #125634188. Canada Post Publications Mail (Canadian Distribution) Agreement Number 1445669. Printed in USA.

Editorial: Unless otherwise stated, bylined articles, as well as product and service descriptions, reflect the author's or firm's opinion. Inclusion in IT Professional does not necessarily constitute endorsement by the IEEE or the Computer Society. All submissions are subject to editing for style, clarity, and space.

WEP vulnerability to attack

An attacker who captures 802.11b data frames possesses the plaintext, the ciphertext, and the initialization vector (IV) used to turn the plaintext into ciphertext. Because WEP uses RC4 encryption, this is enough information to derive the RC4 key stream—the stream of bits XORed with plaintext to generate ciphertext. Knowing a legitimate IV and key stream lets the attacker successfully respond to any future challenge without having to know the actual shared key. Consequently, the attacker has a free pass to join the WLAN, according to the UC Berkeley researchers.

The story is just as bleak for encryption, where the deficiency of the WEP encapsulation design arises because it adapts the RC4 encryption into an environment for which it is poorly suited (Jesse R. Walker, "Unsafe at Any Key Size; An Analysis of the WEP Encapsulation," 27 Oct. 2000, http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip). A group at the University of Maryland (William A. Arbaugh, Narendar Shankar, and Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes," 30 Mar. 2001, http://www.cs.umd.edu/~waa/wireless.pdf) and Cisco (Cisco Comments on Recent WLAN Security Paper from University of Maryland, Product Bulletin No. 1327, Cisco Systems, 1 Nov. 2001, http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm) are also debating these security point.

Testing reveals that WEP encapsulation remains insecure whether its key length is 1 or 1,000 bits. Moreover, the same remains true when any other stream cipher replaces RC4. The weakness stems from WEP's usage of an IV. This vulnerability prevents the WEP encapsulation from providing a meaningful notion of privacy at any key size.

Once again the initialization vector scheme is the source of the problem. By definition, a stream cipher key stream can never be reused, thus obliging the BSS to change the base key as soon as its members have consumed all 2^{24} keys derived from the base key. WEP defines no practical way to change the base key, so in practice, WEP keys are not replaced frequently enough to maintain the intended level of privacy.

A single Access Point BSS running at 11 Mbps with a typical packet distribution can exhaust the derived-key space in about an hour. A campus-wide Access Point network with tens, hundreds, or thousands of stations would exhaust the key space much faster.

Increasing availability of kiddie scripts

At first glance, the complexities of 802.11b security would seem to be daunting for any but the most talented potential hacker. In fact, a readily available hacker script called AirSnort automates the process of breaking into wireless networks (John Leyden, "Tool Dumbs Down Wireless Hacking," *The Register*, 14 Sep. 2001, http://www.theregister.co.uk/content/55/21177.html). Hackers are also purportedly developing a similar script, WEPcrack.

Both tools would let even the most casual hacker exploit the inherent weaknesses in the 802.11b security framework. All a potential digital intruder needs to break into the typical WLAN is a laptop computer, an 802.11b wireless-network card, one of these kiddie scripts, and a parking lot or park bench that is close enough to the building to enable access to the wireless network.

In this brief overview of 802.11b technology, I've painted a fairly gloomy picture of the security you can expect in a WLAN. However, all is not lost: In my next article, I will discuss some architectural strategies you can use to mitigate these security shortcomings. ■

***Joseph Williams** is Practice Manager, Americas, for Sun Microsystems' Advanced Internet Practices group. The information presented here represents the author's opinions and not necessarily those of Sun Microsystems. Contact Williams at joseph.williams@sun.com.*

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