Wireless Security

Models, Threats, and Solutions

Randall K. Nichols
Panos C. Lekkas

McGraw-Hill
New York Chicago San Francisco Lisbon London
Madrid Mexico City Milan New Delhi San Juan Seoul
Singapore Sydney Toronto

Cataloging-in-Publication Data is on file with the Library of Congress.

McGraw-Hill
A Division of The McGraw-Hill Companies

1 2 3 4 5 6 7 8 9 0 DOC/DOC 0 7 6 5 4 3 2 1

ISBN 0-07-138038-8

The sponsoring editor for this book was Marjorie Spencer and the production supervisor was Sherri Souffrance. It was set in ITC Century by MacAllister Publishing Services, LLC.

Printed and bound by R.R. Donnelley & Sons.

CHAPTER

7

The Wireless Local Area Network (WLAN)

A *wireless local area network* (WLAN) is a flexible data communications system implemented as an extension to, or as an alternative for, a wired LAN. WLANs transmit and receive data over the air via RF technology, minimizing the need for any wired connections, and in turn, combining data connectivity with user mobility.[1] WLANs provide all the functionality of WLANs without the physical constraints, and configurations range from simple peer-to-peer topologies to complex networks offering distributed data connectivity and roaming. Besides offering end-user mobility within a networked environment, WLANs enable physical network portability, allowing LANs to move with users that make use of them.

The tradeoff for flexibility and mobility is more threats from hackers using portable computing devices or scanners to intercept data or gain access to the LAN. Unwired LANs are more susceptible to attacks by outside forces via the Internet than wired LANs are. A hacker can crack a network from the convenience of his or her car parked nearby the location of the WLAN. IEEE 802.11, the WLAN standard, provides reliable transfer of wireless data but is vulnerable to hacking or eavesdropping.[2]

In fourth quarter 1999 and first quarter 2000, a collection of reputable vendors brought to market a host of 802.11b-compliant products. The void that IT managers had been facing was finally filled with high speed, interoperable, insecure, and lower-cost wireless equipment.[3] Many IT operations justified the loss of security on the tradeoff for ways to inject mobility, flexibility, and scalability into their networks.

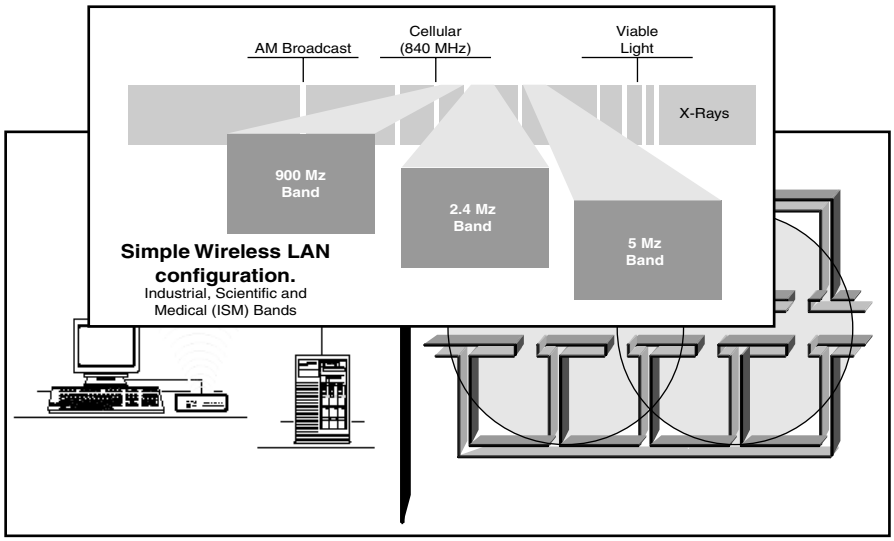
WLANs eliminate the physical link to the network, allowing users to connect directly to a distribution system without interconnecting wires and cables. The network backbone is no longer hidden behind walls and floors nor need it be anchored to a particular physical location. With a WLAN in place, an office infrastructure may be peripatetic, and free to grow and move to suit the needs of the organization.

To say that WLANs are completely without wires would not be strictly correct. Unless a piece of equipment is battery-powered, there must be a power cable connection, and a typical configuration has one or more fixed access points that are connected to a LAN via a traditional data cable. The access points broadcast to and receive information from wireless clients that are within the transmission range. Under ideal circumstances, assuming an environment with few obstructions, the coverage area for a single access point can reach up to several hundred feet and support a small group of users without introducing noticeable performance degradation.

In its simplest form, a WLAN comprises a single transceiver, called an *access point* (AP), that is connected to a wired network via an Ethernet cable as shown in the left frame of Figure 7-1. Access points exist at fixed locations throughout the organization and serve as communications beacons. Network clients with a wireless network adapter installed are able to facilitate data transfer from client to access point and thus from client to server. Introducing more access points near the coverage boundaries of previously deployed broadcast units can extend a wireless network's range. Functioning in a manner similar to cellular telephones, WLANs communicate within cells. Overlapping cells at their perimeters, as depicted in the right frame of Figure 7-2, enables network administrators to extend coverage areas. As clients "roam" around the office, they move from cell to cell, maintaining a connection at all times.

Wireless Transmission Media

Wireless LANs employ *radio frequency* (RF) and *infrared* (IR) electromagnetic airwaves[4] to transfer data from point to point. The *Federal Communications*



7-1 WLAN overview. (courtesy of *Wireless LAN Alliance*)

Commission (FCC) and a general world agreement set aside the radio frequencies that are available for unlicensed commercial use. These *Industrial Scientific and Medical* (ISM) bands include the 900-MHz, 2.4-GHz, and 5-GHz bands that are used by many commercial wireless communication devices. The majority of emerging WLAN devices are designed to operate in the 2.4-GHz band due to global availability and reduced interference.[5]

Several transmission mediums are capable of transferring data across airwaves. Like most technologies, they each have their own benefits and limitations. Infrared systems and narrowband radio systems are the leading technologies being used by the wireless industry.

Infrared Systems

While capable, infrared (IR) systems do not make for a practical enterprise WLAN solution and therefore are not widely employed, IR is able to transfer data by taking advantage of those frequencies located in close proximity to, but beneath visible light on the electromagnetic spectrum. These high bands face the same limitations as visible light in that they cannot penetrate nontransparent objects such as walls, floors, and ceilings. As a result, WLANs transmitting via IR are restricted to operating, at best, within the same room, and could be further limited to a short-range line-of-sight restriction.[6]

Narrowband Radio Systems

Narrowband radio systems transmit and receive data on a specific radio frequency. Different users communicate on alternative frequencies or channels to ensure some level of privacy and avoid interference. Radio receivers are constructed to listen only for their designated frequency and to filter out all others. The natural limitation to this system should be clear: If another transceiver is operating at the same frequency and within range, interference will occur and data will no doubt be lost or corrupted. Another downside of implementing narrowband technology is that, at least in the United States, a license must be obtained from the FCC for each site where it is to be implemented.

Wideband Radio Systems: Spread Spectrum

Instead of using a single frequency, the Spread-Spectrum technology, as its name suggests, traverses the frequency band to reliably transmit data. Originally employed by the military, Spread Spectrum distributes the signal over a wide range of frequencies uniformly, thus consuming more bandwidth in exchange for reliability, integrity, and security of communications. This so-called wideband usage lets devices avoid interference and other signal noise in a way not possible with narrowband transmissions. The benefits come with a price. By their nature, wideband communications are noisier and therefore easier to detect; luckily, to an improperly tuned receiver a Spread-Spectrum signal appears as nothing more than background noise.[7]

Spread Spectrum comes in two forms: *Frequency-Hopping Spread Spectrum* (FHSS) and *Direct-Sequence Spread Spectrum* (DSSS). Of the two, frequency-hopping is less costly to deploy; however, direct-sequence has the potential for more

widespread use. This can be attributed to the higher data rates, greater range, and built-in error correction capabilities of DSSS.

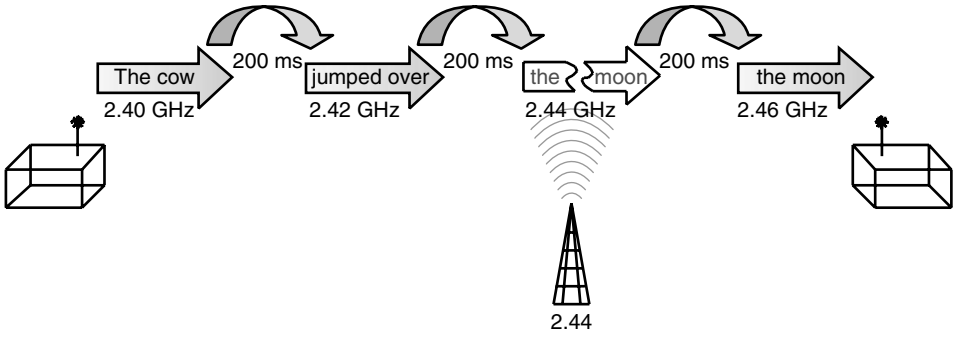
Frequency-Hopping Spread Spectrum (FHSS)

FHSS successfully mitigates the effects of interference by attaching the data signal to a shifting carrier signal. This modulated carrier signal literally hops, as a function of time, from one frequency to the next across the band. Each transceiver is programmed with a hopping code that defines the order and range of frequencies used. To properly communicate, each device must be configured with the same hopping code to ensure that signals are sent and received at the correct time and on the proper frequency.[8] As a result, synchronized transceivers effectively create a logical communications channel with data rates reaching 2 to 3 Mbps and a range of 1,000 feet without installing repeaters.[9]

For interference to occur, the conflicting narrowband signal would need to be broadcast at the same frequency and at the same time as the hopping signal. Should errors in transmission occur on one frequency, the signal will be re-broadcast on a different frequency at the next hop, as shown in Figure 7-2. To receivers that are not programmed with the appropriate hopping code, FHSS transmissions appear to be short duration impulse noise.[10] Distinct hopping codes can be implemented on the same WLAN to prevent sub-WLANs from interfering with one another. FHSS-based WLANs are best for supporting a high number of clients when ease-of-installation is key and either outdoors or in relatively open indoor facilities.[11]

Direct-Sequence Spread Spectrum (DSSS)

DSSS infuses a redundant bit pattern into each bit being transferred. The inserted bits are referred to as a chip or a chipping code.[12] By including the chip, a receiver is able to perform data recovery routines on signals based on statistical analysis. A greater number of bits in the chipping code will result in a signal that is less likely to be negatively affected by interference. As it is increasing the signal size, DSSS requires more bandwidth to operate, generally using three non-overlapping frequen-



7-2 Frequency Hopping Spread Spectrum (FHSS). (Courtesy of *Anyware Network Solutions*)

cies to communicate. The error-correcting capability prevents DSSS from needing to retransmit data that may have been corrupted while en route, as shown in Figure 7-3.

Recall that FHSS systems countered interference by trying to avoid signal collisions through constant motion, essentially attempting to out-pace conflicts. While this is a successful method, it limits data throughput to relatively small packets because the modulation technique has adverse affects on larger data rates. To compensate, DSSS systems include error-correcting bits, thus removing the need to hop frequencies and to retransmit in the event of an error. As a result data rates up to 11 Mbps and ranges up to several miles can be achieved with DSSS.[13]

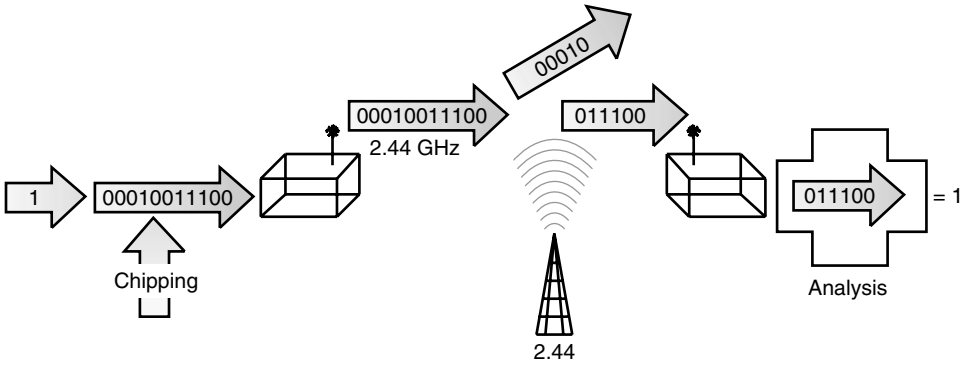
WLAN Products and Standards—Today's Leaders?

The majority of the products from the United States support the IEEE 802.11b standard for WLANs, while European companies are producing devices based on the HyperLan II standard. 802.11 has been in use for many years in one form or another. It has generally been regarded as, at best, moderately secure, but it has never had to face the range of threats we anticipate for WLANs. Recent cryptographic reports on its security indicate that it is seriously flawed.[14]

In the WLAN standards arena, we find security described over and over as an *option*. Although it is paid appropriate deference in all the WLAN assessments, security is understood first as an impediment to increased data transmission and second as appropriate protection. The onus of security is clearly on the user, although the refinements in more recent standards include security enhancements.

802.11 Security?

IEEE 802.11 provides for security through authentication and encryption. In the Ad Hoc or Extended Service Set network mode, authentication can be either open system or shared key. A network station that receives a request may grant authentication to



7-3 Direct-Sequence Spread Spectrum (DSSS). (Courtesy of *Anyware Network Solutions*)

any request or only to those stations on a defined list. In a shared key system, only those stations that possess an encrypted key will receive authentication.[15]

IEEE 802.11 specifies an optional encryption capability called *Wired Equivalent Privacy* (WEP). As the name indicates, the intent is to establish security commensurate to wired networks. WEP employs the RC4 algorithm from RSA Data Security. The RC4 algorithm encrypts over-the-air transmissions.

The security dilemma for 802.11 is that WEP encryption capability does not extend to end-to-end transmission. It protects only the data packet information and does not protect the physical layer header so that other stations on the network can listen to the control data needed to manage the network. (Presumably the other stations cannot decrypt the data portions of the packet.[16])

IEEE 802.11b

Like its predecessor, 802.11b works in the 2.4- to 2.48-GHz band and aims at providing users with connectivity in any country. It also addresses both Ad Hoc and Extended Service Set networks.

Unlike 802.11, though, the IEEE 802.11b removes FHSS as a data transmission mode and establishes DSSS as the standard transmission technology. It does so because DSSS handles weak signals well. With DSSS, data can be extracted from a background of interference without having to be retransmitted. With DSSS as the selected transmission technique, the 802.11b standard also establishes data rate speeds of 5.5 and 11 Mbps.

Some 802.11b-compliant equipment offers an *optional* 128-bit encryption scheme, up from its predecessor's 40- and 64-bit encryption scheme. Also, vendors are producing 802.11b equipment with *network interface cards* (NICs) that possess a unique MAC address and a unique public- and private-key pair. With these enhancements, WLAN administrators can require all hardware address and public-key combinations be entered into the access points (APs) before the network is established, or they can configure the access points to keep track of the combinations they encounter and reject any mismatches. By doing this, an administrator can prevent an attacker from breaking into a network via MAC address spoofing.[17]

Securing WLANs

A WLAN operates in the same manner as a wired LAN except that data is transported through a wireless medium—usually radio waves—rather than cables. Accordingly, a WLAN harbors many of the same vulnerabilities as a wired LAN, plus some that are specific to it. This section discusses common threats facing WLANs, some of the countermeasures that have been designed to address those threats, and the strengths and limitations of those countermeasures.

Eavesdropping

The principal threat is the potential for unauthorized parties to eavesdrop on radio signals sent between a wireless station and an AP, compromising the confidentiality

of sensitive or proprietary information. Eavesdropping is a passive attack. When a radio operator sends a message over a radio path, all other users equipped with a compatible receiver within the range of the transmission can listen to the message. Furthermore, because an eavesdropper can listen to a message without altering the data, the sender and intended receiver of the message may not even be aware of the intrusion.[18]

Wired LANs are also vulnerable to eavesdropping, but not to the same extent. A wired LAN may radiate electromagnetic signals through cabling, but an eavesdropper must be close to the cabling to hear the signals with a listening device. By contrast, someone eavesdropping on a WLAN may be located some distance from the network and may even be outside the physical confines of the environment in which the network operates. This is because radio signals emitted from a WLAN can propagate beyond the area in which they originate, and can penetrate building walls and other physical obstacles, depending on the transmission technology used and the strength of the signal.

Equipment capable of intercepting WLAN traffic is available to consumers in the form of wireless adapters and other 802.11-compatible products. The difficulty for eavesdroppers is to decode a 2.4-GHz digital signal because most WLAN systems use Spread-Spectrum technology, which is resistant to eavesdropping. In addition, if encryption is used, eavesdroppers must decipher encrypted content. Despite these difficulties, eavesdropping poses a significant threat to WLAN communications.

Unauthorized Access

A second threat to WLAN security is the potential for an intruder to enter a WLAN system disguised as an authorized user. Once inside, the intruder can violate the confidentiality and integrity of network traffic by sending, receiving, altering, or forging messages.[19] This is an active attack, and may be carried out using a wireless adapter that is compatible with the targeted network, or by using a compromised (for example, stolen) device that is linked to the network.

The best protection against unauthorized access is to deploy authentication mechanisms to ensure only authorized users can access the network. Such mechanisms are regularly deployed on wired LANs, not only to prevent unauthorized access, but also to detect intrusions when they occur. Discovering intruders attempting to access a WLAN isn't easy. This is because unsuccessful attacks might be misinterpreted as unsuccessful logon attempts caused by the high *bit error rate* (BER) of radio transmissions or by stations belonging to another WLAN.[20]

A variant of unauthorized access is an attacker who deceives wireless stations by setting up a counterfeit AP. When a wireless station is first powered on or when it enters a new microcell, it chooses an AP to link to, based on signal strength and observed packet error rates. If accepted by the AP, the station tunes to the radio channel that the AP is using. By setting up a counterfeit AP with a powerful signal, an attacker might be able to lure a station onto his or her network in order to capture secret keys and logon passwords. Alternately, the attacker may reject the logon attempts but record the messages transmitted during the logon process, for the same purpose.[21]

The first type of attack described above is very difficult to implement, because the attacker must have detailed information to be able to trick the station into

believing that it has accessed its home network. Otherwise, the attack may be easily detected. The second type of attack is easier to implement, because the attacker only requires a receiver and an antenna that is compatible with targeted stations. This attack also is more difficult to detect because unsuccessful logons are relatively common in WLAN communications. The best protection against both types of attacks is to use an efficient authentication mechanism that enables wireless stations to authenticate to APs without revealing secret keys or passwords.[22]

Interference and Jamming

A third threat to WLAN security is radio interference that can seriously degrade bandwidth (data throughput). In many cases interference is accidental. Because WLANs use unlicensed radio waves, other electromagnetic devices operating in the infrared or 2.4-GHz radio frequency can overlap with WLAN traffic. Potential sources of interference include high-power amateur, military, and *industrial, scientific, and military* (ISM) transmitters. Microwave ovens are a possible source, but most WLAN vendors design their products to minimize microwave interference. Another concern is the operation of two or more WLANs in the same coverage area; some WLANs are designed to operate in close proximity to other systems while others are not.[23]

Of course interference may also be intentional. If an attacker has a powerful transmitter, he or she can generate a radio signal strong enough to overwhelm weaker signals, disrupting communications. This is a condition known as jamming,[24] and is a denial-of-service attack. Two types of jammers that may be used against WLAN traffic are high-power pulsed full-band jammers that cover the entire frequency used by the targeted signal, and lower-power partial-band jammers that cover only part of the frequency used by the targeted signal.[25]

Jamming equipment is readily available to consumers or can be constructed by knowledgeable attackers. In addition, jamming attacks can be mounted from a location remote from the targeted network (for example, from a vehicle parked across the street, or an apartment in the next block). Direction-finding equipment can detect the source of jamming signals, but not necessarily in time to prevent the jamming.[26]

Physical Threats

WLANs can be brought down by damage to or destruction of the underlying physical infrastructure. Like a wired LAN, a WLAN operating in infrastructure mode relies on a variety of physical components, including APs, cables, antennas, wireless adapters,[27] and software. Damage to any of these components could reduce signal strength, limit coverage area, or reduce bandwidth, hampering the ability of users to access data and information services (for example, file servers, printers, and Internet links). If severe enough, compromise of the physical infrastructure could even shut down WLAN operations.

Infrastructure components are susceptible to the conditions of the environment in which they operate, especially if it's outdoors. APs can be obstructed by snow, ice, and distorting radio signals. Antennas mounted atop poles or buildings can be knocked askew by winds or bent by ice, changing the angle of the beam width used

for transmitting signals. This can be especially problematic for antennas with narrow beam widths, such as parabolic dish antennas.[28] Antennas and APs can also be damaged by nearby lightning strikes or water intrusion into the cabling and connectors linking it to the wired network.[29] Finally, accidents and improper handling can damage wireless adapters and wireless stations.

Physical components may also be subject to attack. WLANs generally rely on a smaller physical plant than do wired LANs, making them less vulnerable to sabotage, but they are not entirely safe. For example, an attacker could cut the cabling that connects an AP to the wired network, isolating affected microcells and disrupting power to the receiver. An attacker might also be able to damage or destroy an exposed AP or the antenna connected to it. An attacker might also steal or compromise a wireless station or adapter and use it to try to intercept WLAN traffic or to gain unauthorized access to the network. Finally, an attacker could avoid the WLAN altogether and instead sabotage the wired network, disrupting the operation of all WLANs connected to it.[30]

Countermeasures

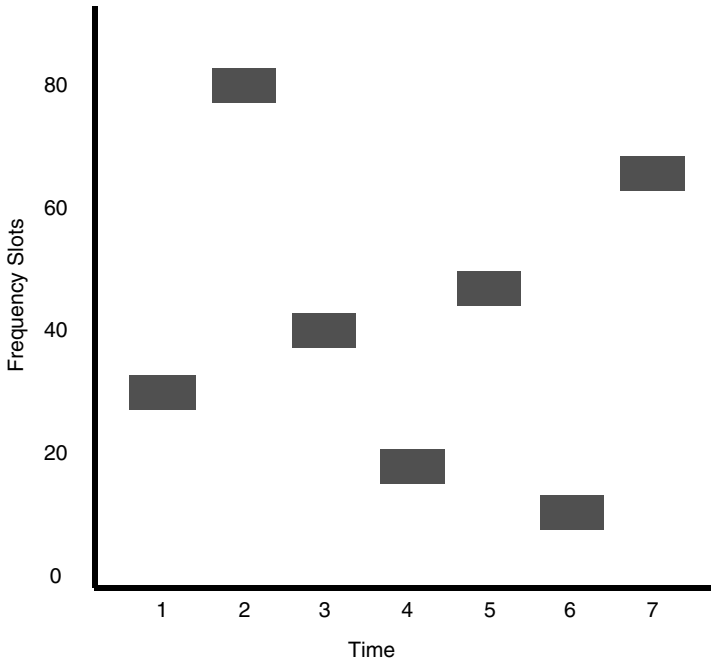
WLAN systems most commonly use Spread-Spectrum technology to transmit data. Spread Spectrum is designed to resist eavesdropping, interference, and noise. To the casual listener, the signal sounds like random background noise. Spread Spectrum consumes more bandwidth than do narrowband transmissions (which concentrate signals into a single frequency), but it produces a signal that is easy to detect if the receiver knows the parameters of the transmission. The receiver uses the same spreading code used by the transmitter to regroup the spread signal to its original form.[31]

Frequency-Hopping Spread Spectrum (FHSS)

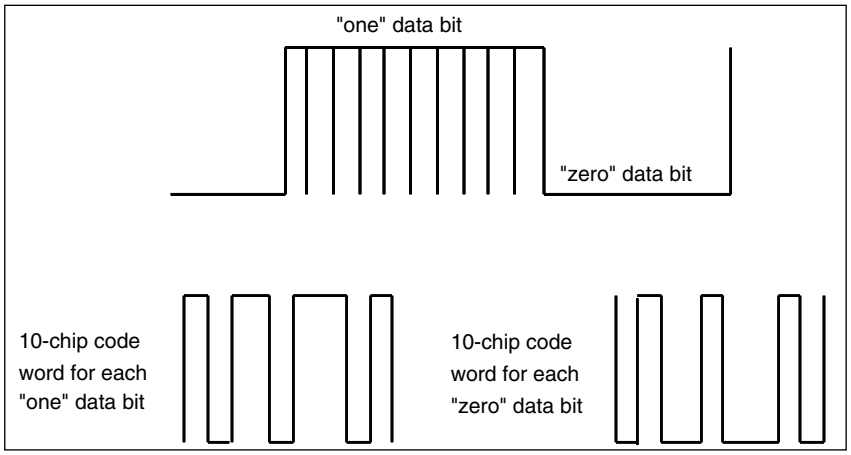
The 2.4-GHz band is divided into 75 one-megahertz channels. A radio signal is sent (hopped) over all 75 frequencies in accordance with a pseudo-random code sequence that is known to both the transmitter and the receiver (see Figure 7-4). The FHSS physical layer has 22 hop patterns; the pattern chosen by the transmitter is taken from a predetermined set specified by the code. The receiver tracks that hopping pattern. When the transmitter and the receiver are properly synchronized, data is transmitted over what is essentially a single channel. To an eavesdropper, the signal appears to be unintelligible short duration impulse noise. In addition, because the signal is spread across multiple frequencies, the potential for interference is minimized.[32]

Direct-Sequence Spread Spectrum (DSSS)

Under the original 802.11 standard, DSSS breaks each data bit in the signal (0 or 1) into 11 sub-bits called chips, which are converted into a waveform (see Figure 7-5). The waveforms are then transmitted over a wide range of frequencies. The receiver unspreads the chip to recover the original data. If one or more bits are lost or damaged during transmission, the receiver can use installed statistical techniques to



7-4 Hopping code. (Source: The Wireless LAN Alliance)[33]



7-5 DSSS Chip Codes. (Source: The Wireless LAN Alliance)[34]

recover the original data. Under the 802.11b standard, DSSS uses 64 8-bit code words to spread the signal. To an eavesdropper or other unauthorized user, a DSSS signal appears as low-power wideband noise. Therefore, most narrowband receivers ignore it. In addition, interference is minimized because the signal is spread over a wide range of frequencies.[35]

Both FHSS and DSSS pose difficulties for outsiders attempting to intercept radio signals. In the case of FHSS, an eavesdropper must know the hopping pattern that is used in the transmission. In the case of DSSS, the eavesdropper must know the chipping code (802.11) or code words (802.11b). In both cases, the eavesdropper must also know the frequency band and modulation techniques in order to accurately read the transmitted signal. Furthermore, radio systems use a form of data scrambling that facilitates the timing and decoding of radio signals. An eavesdropper must also know this scrambling pattern if he or she is to read intercepted data.[36]

Adding to an eavesdropper's difficulties is the fact that Spread-Spectrum technologies do not interoperate with each other (that is, a WLAN using FHSS cannot communicate with WLAN using DSSS, and vice versa). Even if two different systems are using the same technique, they cannot communicate if they are using different frequency bands (for example, a system using DSSS cannot communicate with another system using DSSS if they are operating on different frequencies).[37] Consequently, an eavesdropper cannot use one Spread-Spectrum technique to intercept radio signals transmitted by the other technique. Nor can he or she intercept radio signals without knowing the frequency that is used, even if he or she has an 802.11-compatible receiver.

Despite the ability of Spread-Spectrum technology to resist eavesdropping, it is only secure if the hopping pattern or chipping code is unknown to the eavesdropper; however, these parameters are published in the 802.11 standard, and therefore are public knowledge. The modulation method is also specified. Using this information, a knowledgeable eavesdropper could build a receiver to intercept and read unprotected signals.[38] Nevertheless, the inherent strengths of Spread-Spectrum technology are sufficient to defeat most would-be eavesdroppers and therefore contribute to the security of WLAN communications.

Spread-Spectrum technology also minimizes the potential for interference from other radios and electromagnetic devices by spreading radio transmissions over a wide range of frequency bands. Nevertheless, it is vulnerable to jamming. Depending on the type of jammer used, errors are produced at the demodulator output, disrupting affected signals. In general, FHSS tends to be more effective than DSSS against narrowband jamming and partial-band noise jamming, because the jamming tends to corrupt only a fraction of the hopped code. With DSSS, all codes are corrupted to some extent by the jamming signal. In addition, FHSS spreads signals over a wider range of frequencies than DSSS does.[39]

Two other technologies used in some WLAN systems are infrared and narrowband, described in the following section. Both technologies lack the robustness of Spread Spectrum to resist eavesdropping and interference.

Infrared (IR)

IR is the third radio technology specified in the original 802.11 standard. IR transmits data at very high frequencies that are just below visible light on the electromagnetic spectrum. Like light, IR cannot penetrate walls and other solid or opaque objects; the transmitter and receiver must have direct line-of-sight or else use diffuse technology. Low-power IR systems have limited range (approximately three feet for most computers). High-power IR systems can transmit radio signals over longer ranges, but poor weather conditions and the requirement for direct line-of-sight minimize the effectiveness of these systems for mobile users. In addition, IR signals transmitted in the open are vulnerable to interception, interference, and jamming. Consequently, IR systems typically are used for high-security applications in enclosed facilities. IR systems also tend to be more expensive than FHSS and DSSS systems, and the data rate is low at one to two Mbps. The result is that IR systems are used in few commercial WLAN products.[40]

Narrowband

Some WLAN products use narrowband technology that transmits and receives radio signals on a specific frequency. The effect is to keep the radio signal as narrow as possible. Cross-talk among radio channels is prevented by coordinating different channel frequencies among different users. The receiver tunes only to those signals on its designated frequency and rejects all others. The drawback of narrowband is that eavesdroppers can easily detect transmitted signals, and it is vulnerable to interference and jamming. In addition, narrowband requires a license from the Federal Communications Commission (FCC) for each site where it is used, unlike Spread-Spectrum technologies that do not require FCC licensing.[41]

The Infamous WEP

Although WLAN systems can resist passive eavesdropping, the only way to effectively prevent third parties from compromising transmitted data is to use encryption. The purpose of WEP is to ensure that WLAN systems have a level of privacy that is equivalent to that of wired LANs by encrypting radio signals. A secondary purpose of WEP is to prevent unauthorized users from accessing WLANs (that is, provide authentication). This secondary purpose is not explicitly stated in the 802.11 standard, but it is considered an important feature of the WEP algorithm.[42]

WEP is a critical element for securing the confidentiality and integrity of data on 802.11-standard-based WLAN systems, as well as for providing access control through authentication. Consequently, most 802.11-compliant WLAN products support WEP as either a standard or an optional feature. The manner in which WEP provides encryption and authentication is described next.

Encryption

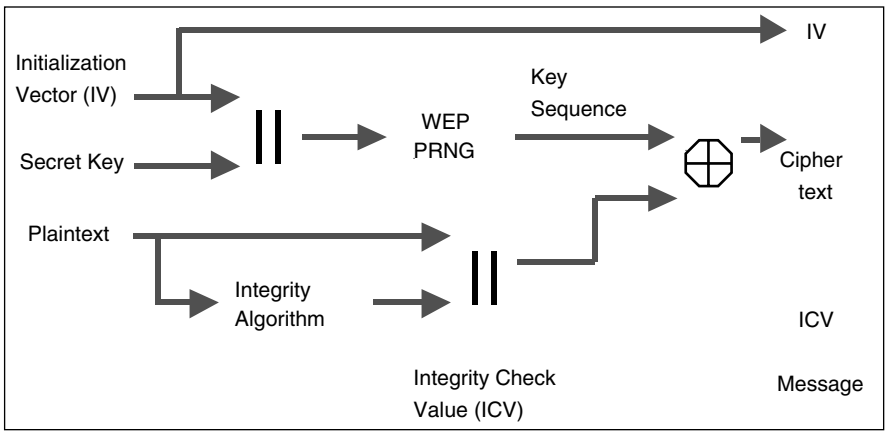
WEP uses a secret key that is shared between a wireless station and an access point (AP). All data sent and received between a wireless station and an AP may be encrypted using this shared key. The 802.11 standard does not specify how the

secret key is established, but it does allow for an array that associates a unique key with each station. In general practice, however, one key is shared among all stations and APs in a given system.

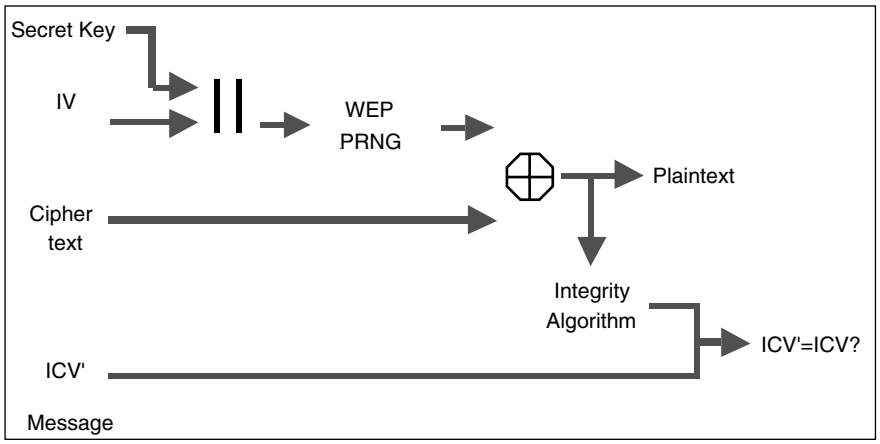
WEP provides data encryption using a 40-bit (weak) [802.11] or 128-bit (strong)[802.11b] secret key and a RC4 *Pseudo Random Number Generator* (PRNG). Two processes are applied to plaintext data: one encrypts the plaintext, and the other protects it from unauthorized modification while it is in transit. The secret key is concatenated with a random *initialization vector* (IV) that adds 24 bits to the resulting key. This key is inserted into the PRNG that generates a long pseudo-random key stream. The sender XORs the key stream with the plaintext to generate encrypted text, or ciphertext, and transmits it to the receiver along with the IV. Upon receipt of the ciphertext, the receiver uses the IV and its own copy of the secret key to produce a key stream that is identical to the key stream generated by the transmitter. The receiver then XORs the key stream with the ciphertext to reveal the original plaintext.[43]

To protect the ciphertext against unauthorized modification while in transit, WEP applies an integrity check algorithm (CRC-32) to the plaintext, which produces an *Integrity Check Value* (ICV). The ICV is then concatenated to the plaintext. The ICV is in effect the fingerprint of the plaintext. The ICV is attached to the ciphertext and sent to the receiver along with the IV. The receiver combines the ciphertext with the key stream to uncover the plaintext. Applying the integrity algorithm to the plaintext and comparing the output IVC to the transmitted ICV verify the decryption. If the two ICVs are identical, the message is authenticated; that is, the fingerprints match.[44] Figures 7-6 and 7-7 illustrate WEP encryption and decryption, respectively.

Despite the potential strength of WEP for protecting the confidentiality and integrity of data, it has limitations that can only be addressed by proper management. The first problem stems from the reuse of the IV. The IV is included in the



7-6 WEP encryption. (Source: Sultan Weatherspoon, "Overview of IEEE 802.11b Security," *Intel Technology* Journal, Quarter 2, 2000)



7-7 WEP decryption. (Source: Weatherspoon, "Overview of IEEE 802.11b Security")

unencrypted part of a message so the receiver knows what IV to use when generating the key stream for decryption. The 802.11 standard recommends—but does not require—that the IV be changed after each transmission. If the IV is not changed regularly, but is reused for subsequent messages, an eavesdropper may be able to cryptanalyze the key stream generated by the IV and secret key and thus decrypt messages that use that IV.[45]

The problem of IV reuse potentially leads to another. Namely, once an attacker knows the key sequence for an encrypted message, based on a reused IV, he or she can use this information to build an encrypted signal and insert it into a network. The process is to create a new message, calculate the CRC-32, and modify the original encrypted message to change the plaintext to the new message. The attacker can then transmit the message to an AP or wireless station, which would accept it as a valid message. Changing the IV after each message is a simple way to prevent both this problem and the issue described previously.[46]

Key distribution is another problem. Most WLANs share one key among all stations and APs in the network. It is unlikely that a key shared among many users will remain secret indefinitely. Some network administrators address this problem by configuring wireless stations with the secret key themselves, rather than permitting end users to perform this task. That's an imperfect solution; however, because the shared key is still stored on the users' computers where it is vulnerable. In addition, if a key on even one station is compromised, all the other stations in the system must be reconfigured with a new key. The better solution is to assign a unique key to each station and to change keys frequently.[47]

Although WEP encryption is designed to be computationally efficient, it can reduce bandwidth in use. According to one report, 40-bit encryption reduces bandwidth by 1 Mbps, and 128-bit encryption reduces bandwidth by 1 to 2 Mbps. This degree of drop is relatively small, but users may still notice it, especially if the signal

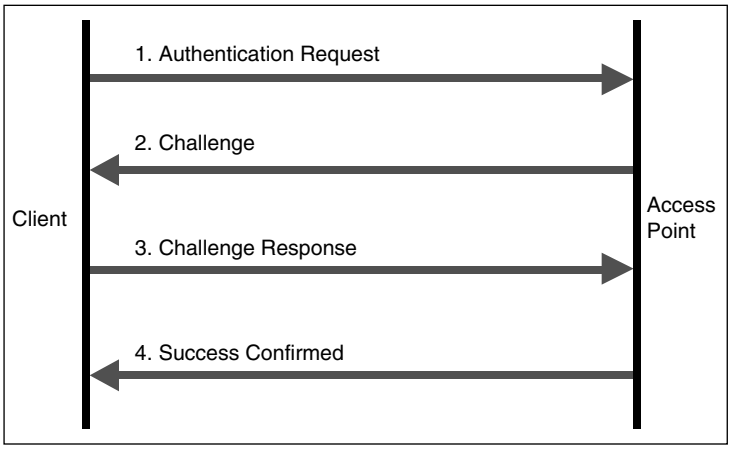
is transmitted via FHSS, which transmits signals at a maximum of only 3 Mbps. In many cases, the exact impact will depend on the product that is used and number of users on the system.[48]

Authentication

WEP provides two types of authentication: a default Open System, whereby all users are permitted to access a WLAN, and shared key authentication, which controls access to the WLAN and prevents unauthorized network access. Of the two levels, shared key authentication is the secure mode. It uses a secret key that is shared among all stations and APs in a WLAN system. When a station tries to associate with an AP, the AP replies with random text by way of a challenge. The station must use its copy of the shared secret key to encrypt the challenge text and send it back to the AP in order to authenticate itself. The AP decrypts the response using the same shared key and compares it to the challenge text sent earlier. If the text is identical, the AP sends a confirmation message to the station and accepts the station into the network. If the station does not have a key, or if it sends the wrong response, the AP rejects it, preventing the station from accessing the network.[49] Shared key authentication is illustrated in Figure 7-8.

Note that shared key authentication works only if WEP encryption is enabled. If it is not enabled, the system will default to the Open System mode, permitting almost any station within range of an AP to access the network.[50] That creates a window for an intruder into the system, where he or she may send, receive, alter, or forge messages. Make sure that WEP is enabled whenever secure authentication is required.

Even when shared key authentication is enabled, all wireless stations in a WLAN system may have the same shared key, depending on how the system is installed. For such systems, individual authentication is not possible; all users—including unauthorized ones—with the shared key can access the network. This weakness can



7-8 Shared key authentication. (Source: Sultan Weatherspoon, "Overview of IEEE 802.11b Security," *Intel Technology* Journal, Quarter 2, 2000)

result in unauthorized access, especially if the system includes a large numbers of users. The more users, the greater the likelihood that the shared key could fall into the wrong hands.

Finally, in many WLAN systems, the key used for authentication is the same key used for encryption. This particular weakness compounds the problems described previously. If an attacker has the shared key, he or she can use it to not only to access the network but also to decrypt messages, thus creating a dual threat. The solution is to distribute separate keys throughout the system—one for authentication and another for encryption.

Wired Equivalency Protocol Flaws Too Public

WEP has been found to be highly (albeit spectacularly) flawed, to the serious detriment of its security claims and supporters. WLANs have be successfully subjected to various forms of attack, including decryption, based upon statistical analysis. WEP has the additional vulnerability of ignoring some unauthorized traffic or an unauthorized decryption, injected by an attacker tricking the access point.[51] Because of these drawbacks, it's likely that WEP will be used in the future only in conjunction with VPNs.

Other Authentication Techniques

It's reasonable to consider authentication techniques other than shared key authentication. *Extended Service Set Identification* (ESSID) is a commonly used access control technique. ESSID is a value programmed into each AP to identify which subnet the AP is on. This value can be used for authentication to ensure that only authorized stations can access the network. If a station does not know the ESSID, it is not permitted to associate with the AP.[52]

In addition, some manufacturers provide for a table of *Media Access Control* (MAC) addresses in an *access control list* (ACL) that is included in the AP. When a station tries to associate with the AP, the router in the AP reads the unique MAC address on the station's wireless adapter and determines whether it is on the ACL. Access to the network is restricted to those stations on the list; others are rejected. This enables network administrators to include or exclude wireless stations.[53] This capability provides a valuable layer of additional security, not only to exclude outside stations but also to exclude those stations that belong to the network but have been compromised (for example, a stolen computer).

Physical Security

Precautions must be taken to protect the physical components of a WLAN from accidents, weather, and vandalism. Those precautions should be commensurate with the type of risks to which the components are exposed, the probability that these risks will occur, and the impact that an occurrence would have on WLAN operations. If the equipment cannot be adequately protected, it should be hardened to minimize the impact of these conditions. APs and antennas should be securely mounted and located in areas that minimize their exposure to potential sources of interference,

including microwave ovens and other transmitters. If outdoors, APs and antennas should be situated to minimize exposure to high winds, snow, and ice, or else they should be properly sheltered. Lightning arrestors should be deployed to suppress the effect of lightning strikes. Cabling should be housed in protective covering, where possible, and nearby pipes and water tanks should be properly maintained to prevent leaks and accidental spills.[54]

In addition, unauthorized personnel should be denied access to WLAN equipment. Locate APs and antennas in securable areas, away from the public traffic and protected with appropriate barriers and access controls. Intrusion detection systems such as closed-circuit television may also be used to monitor remote or exposed assets.

Along with physical measures, employ appropriate administrative controls. Wireless stations assigned to WLAN users should be properly logged and the identity of the users recorded. ACLs should be maintained and regularly updated. WLAN equipment should be properly labeled to ensure identification if it is damaged or destroyed. Labeling may also deter theft. Response procedures should be developed in the event that WLAN equipment is compromised, damaged, or destroyed.

Finally, users should be educated on the importance of protecting their stations from theft, damage, and misuse. For example, users should never leave their stations unattended in public areas, and they should log out from the network if they are not using it. In addition, users should not eat or drink near their station, and they should avoid working near possible hazards, such as microwave ovens. They should also immediately report any occurrence of suspicious activity involving the WLAN, including all cases of compromised or stolen equipment.

Summary

Despite the advantages of wireless networking, WLANs are vulnerable to security threats. Common threats include eavesdropping, unauthorized access, interference and jamming, and physical damage. Depending on how a WLAN is designed or configured, such threats may be prevented or mitigated. For example, systems that use Spread-Spectrum technology are resistant to passive eavesdropping and interference. Systems that use the WEP encryption algorithm are resistant to active eavesdropping and provide client authentication. If WEP is employed, however, measures must be taken to ensure that encryption keys are properly managed. Finally, the physical components of a WLAN can be protected from damage by installing physical safeguards and providing training to users.

Endnotes

[1]"How will WAP work with GPRS?" http://wap.com/cgi-bin/wapfaq.cgi?chapter=9.4, 1 February 2001.

[2]"The IEEE 802.11 Standard, Wireless LAN Standard," http://www.wlana.org/learn.

[3]"Enterprise Wireless LAN Market Update," http://www.instat.com/abstracts/ln/2000/ln0011wl_abs.htm, Cahners In-Stat Group, December 2000.

[4]"What is a Wireless LAN: Introduction to Wireless LANs," www.wlana.com/learn/educate.htm, Wireless LAN Alliance (WLANA). January 1, 2001.

[5]"Wireless Networking: The Next Generation," Cisco Systems, Inc., 2000 (CD-ROM).

[6]"What is a Wireless LAN," http://www.wirelesslan.com/wireless/, WirelessLAN.com Answer Page, September 28, 1999.

[7]Ibid.

[8]Geier, Jim, "Spread Spectrum: Frequency Hopping vs. Direct Sequence," http://www.wireless-nets.com/whitepaper_spread.htm, May 1999.

[9]"Wireless LAN Technical Overview," http://www.anyware-ns.com/technical_overview.htm, Anyware Network Solutions, January 9, 2001.

[10]"What is a Wireless LAN: Introduction to Wireless LANs," www.wlana.com/learn/educate.htm, Wireless LAN Alliance (WLANA), January 1, 2001.

[11]"Wireless LAN Technical Overview," http://www.anyware-ns.com/technical_overview.htm, Anyware Network Solutions, January 9, 2001.

[12]"What is a Wireless LAN: Introduction to Wireless LANs," www.wlana.com/learn/educate.htm, Wireless LAN Alliance (WLANA), January 1, 2001.

[13]"Wireless LAN Technical Overview," http://www.anyware-ns.com/technical_overview.htm, Anyware Network Solutions, January 9, 2001.

[14]Borisov, Nikita, Ian Goldburg, and David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11 (Draft)," 3.

Borisov, Nikita, Ian Goldburg, and David Wagner, "Security of the WEP Algorithm," www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

Hong Siang, Teo, "Security in Wireless LAN," July 1, 2000, http://202.85.163.46/articles/wireless/WLAN_security.pdf.

Uskela, Sami, "Security in Wireless Local Area Networks," Helsinki University of Technology, www.tml.hut.fi/Opinnot/Tik-110501/1997 /wireless_lan.html.

Weatherspoon, Sultan, "Overview of IEEE 802.11b Security," *Intel Technology Journal* (Quarter 2, 2000), p. 1.

"Wireless LAN Security White Paper," Wireless LAN Alliance (WLANA), 2000, www.wlana.com.

[15]"The IEEE 802.11 Standard, Wireless LAN Standard," http://www.wlana.org/learn.

[16]Ibid.

[17]Ibid.

[18]Borisov, Nikita, Ian Goldburg, and David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11 (Draft)," p. 3.

Borisov, Nikita, Ian Goldburg, and David Wagner, "Security of the WEP Algorithm," www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

Hong Siang, Teo, "Security in Wireless LAN," July 1, 2000, http://202.85.163.46/articles/wireless/WLAN_security.pdf.

Uskela, Sami, "Security in Wireless Local Area Networks," Helsinki University of Technology, www.tml.hut.fi/Opinnot/Tik-110501/1997 /wireless_lan.html.

Weatherspoon, Sultan, "Overview of IEEE 802.11b Security," *Intel Technology Journal* (Quarter 2, 2000), p. 1.

"Wireless LAN Security White Paper," Wireless LAN Alliance (WLANA), 2000, www.wlana.com.

[19]"Wireless LAN Technology for Mobility, Performance and Security," Ericsson Enterprise, www.ericsson.com/wlan/te-security.asp.

[20]Uskela, Sami, "What's New in Wireless LANs: The IEEE 802.11b Standard," 3Com Corporation, 2000, www.3com.com/technology/tech_net/white_papers/503072a.html.

[21]Ibid.

[22]Ibid.

[23]"Which Products Should I Buy?" WirelessLAN.com Answer Page, www.wirelesslan.com/product; and "What is a Wireless LAN: Introduction to Wireless LANs," WLANA, 2000, 8, www.wlana.com.

[24]Muller, Nathan J., *Desktop Encyclopedia of Telecommunications*, 2nd ed., McGraw-Hill, 2000, p. 814.

[25]Feldman, Philip M., "Emerging Commercial Mobile Wireless Technology and Standards: Suitable for the Army?" RAND, 1998, p. 8.

[26]Uskela.

[27]End users access the WLAN through wireless adapters that are installed on their wireless stations. Adapters come in various forms, including PC cards for laptop computers, ISA or PCI adapters in desktop computers, and integrated devices in hand-held computers. *See* "Introduction to Wireless LANs," p. 3.

[28]Telex® Wireless Products Group, "WLAN Antenna: Frequently Asked Questions," www.telexwireless.com/wlanfaq.htm.

[29]Telex® Wireless Products Group.

[30]Although affected users might be able to set up an ad hoc network to continue communications, they would be isolated from the wired network, and therefore probably could not carry on effective operations for an extended period.

[31]Muller, p. 813.

[32]Muller, p. 816, and "What's New in Wireless LANs: The IEEE 802.11b Standard."

[33]www.wlana.com

[34]www.wlana.com

[35]Muller, p. 815; "What's New in Wireless LANs: The IEEE 802.11b Standard," "The IEEE 802.11 Wireless LAN Standard White Paper," WLANA, 2000, www.wlana.com; "What is a Wireless LAN: Introduction to Wireless LAN," p. 6.

[36]van der Merwe, Jacques, "Securing Air," *Infrastructure News*, June 26, 2000, www.computerweek.com, and "Wireless LAN Security White Paper."

[37]Feldman, p. 46.

[38]The Modulation Method for FHSS is 2–4 Level Gaussian FSK, and the Modulation for DSSS is Differential BPSK and DQPSK, See "The IEEE 802.11 Wireless LAN Standard White Paper" and Siang, p. 2.

[39]Feldman, pp. 14–17, 72. Feldman observes, however, that commercial spread spectrum techniques do not use secure spreading sequences, due to key distribution problems, and therefore have no advantage over nonspread (that is, narrowband) systems. In addition, the spreading gains used in commercial systems tend to be much smaller than the spreading gains used in military systems, reducing their ability to resist broadband jamming.

[40]"Wireless LAN Technical Overview," www.anyware-ns.com/technical_overview.htm; "The IEEE 802.11 Wireless LAN Standard White Paper," and "Wireless LAN Security White Paper."

[41]"What is a Wireless LAN: Introduction to Wireless LANs," p. 6.

[42]Borisov, Goldberg, and Wagner, "(In)Security of the WEP Algorithm."

[43]Weatherspoon, p. 2, Borisov, Goldburg, and Wagner, "Intercepting Mobile Communications," p. 2.

[44]Weatherspoon, p. 2;

[45]Borisov, Goldberg, and Wagner, "Intercepting Mobile Communications," pp. 3–4, 7–8; Weatherspoon, p. 3.

[46]Ibid.

[47]Borisov, Goldberg, and Wagner, "Intercepting Mobile Communications," pp. 6, 11.

[48]Brooks, Jason, and Herb Bethoney, "The LAN, PAN, WAN Plan," *eWEEK*, 14 January 2001, http://www1.zdnet.com; and Siang, p. 2.

[49]Weatherspoon, p. 3.

[50]Weatherspoon, p. 3, and Siang, p. 2.

[51]"Wireless LANs Have Serious Flaws, Berkeley Researchers Say," ComputerWorld Magazine, February 12, 2001.

[52]"What's New in Wireless LANs: The IEEE 802.11b Standard."

[53]Ibid.

[54]National Institute of Standards and Technology (NIST), *An Introduction to Computer Security: The NIST Handbook*, pp. 146, 166–167, 170–172.

NIST, SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996, pp. 41–42.

Critical Infrastructure Assurance Office (CIAO), *Practices for Securing Critical Information Assets*, January 2000, pp. 27–29.

NIST, Guidance Federal Information Processing Standards (FIPS) Publications (PUB) 191, *Guidelines for the Analysis of Local Area Network Security*, November 9, 1994, http://www.itl.nist.gov/fipspubs/fip191.htm.