Wireless (In)Security

by Rusty Nejdl
rusty@ringofsaturn.com

Introduction

802.11 refers to a family of specifications developed by the IEEE for wireless lan technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.
There are several specifications in the 802.11 family:

- **802.11** -- applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- **802.11a** -- an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- **802.11b** (also referred to as *802.11 High Rate* or Wi-Fi) -- an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- **802.11g** -- applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band

Frequency Hopping Spread Spectrum

Frequency hopping is one of two basic modulation techniques used in spread spectrum signal transmission. It is the repeated switching of frequencies during radio transmission, often to minimize the effectiveness of "electronic warfare" - that is, the unauthorized interception or jamming of telecommunications. It also is known as frequency- hopping code division multiple access (FH-CDMA).

Spread spectrum modulation techniques have become more common in recent years. Spread spectrum enables a signal to be transmitted across a frequency band that is much wider than the minimum bandwidth required by the information signal. The transmitter "spreads" the energy, originally concentrated in narrowband, across a number of frequency band channels on a wider electromagnetic spectrum. Benefits include improved privacy, decreased narrowband interference, and increased signal capacity.

In an FH-CDMA system, a transmitter "hops" between available frequencies according to a specified algorithm, which can be either random or preplanned. The transmitter operates in synchronization with a receiver, which remains tuned to the same center frequency as the transmitter. A short burst of data is transmitted on a narrowband. Then, the transmitter tunes to another frequency and transmits again. The receiver thus is capable of hopping its frequency over a given bandwidth several times a second, transmitting on one frequency for a certain period of time, then hopping to another frequency and transmitting again. Frequency hopping requires a much wider bandwidth than is needed to transmit the same information using only one carrier frequency.

The spread spectrum approach that is an alternative to FH-CDMA is direct sequence code division multiple access (DS-CDMA), which chops the data into small pieces and spreads them across the frequency domain. FH-CDMA devices use less power and are generally cheaper, but the performance of DS-CDMA systems is usually better and more reliable. The biggest advantage of frequency hopping lies in the coexistence of several access points in the same area, something not possible with direct sequence.

Certain rules govern how frequency-hopping devices are used. In North America, the Industrial, Scientific, and Medial (ISM) waveband is divided into 75 hopping channels, with power transmission not to exceed 1 watt on each channel. These restrictions ensure that a single device does not consume too much bandwidth or linger too long on a single frequency.

The Federal Communications Commission (Fcc) has amended rules to allow frequency hopping spread spectrum systems in the unregulated 2.4 GHz band. The rule change is designed to allow wider bandwidths, thus enabling Internet devices to operate at higher speeds and fostering development of wireless LANs and wireless cable modems.

Movie star Hedy Lamarr is generally credited as co-originator of the idea of spread spectrum transmission. She and her pianist were issued a patent for the technique during World War II. They discovered the technique using a player piano to control the frequency hops, and envisioned it as a way to provide secure communications during wartime. The pair never made any money off the invention and their patent eventually expired. Sylvania introduced a similar concept in the 1950s and coined the term "spread spectrum."

Direct Sequence Spread Spectrum

Direct sequence spread spectrum, also known as direct sequence code division multiple access (DS-CDMA), is one of two approaches to spread spectrum modulation for digital signal transmission over the airwaves. In direct sequence spread spectrum, the stream of information to be transmitted is divided into small pieces, each of which is allocated across to a frequency channel across the spectrum. A data signal at the point of transmission is combined with a higher data-rate bit sequence (also known as a *chipping code*) that divides the data according to a spreading ratio. The redundant chipping code helps the signal resist interference and also enables the original data to be recovered if data bits are damaged during transmission.

Direct sequence contrasts with the other spread spectrum process, known as frequency hopping spread spectrum, or frequency hopping code division multiple access (FH-CDMA), in which a broad slice of the bandwidth spectrum is divided into many possible broadcast frequencies. In general, frequency-hopping devices use less power and are cheaper, but the performance of DS-CDMA systems is usually better and more reliable.

Spread spectrum first was developed for use by the military because it uses wideband signals that are difficult to detect and that resist attempts at jamming. In recent years, researchers have turned their attention to applying spread spectrum processes for commercial purposes, especially in local area wireless networks.

Wireless LAN Standards

Use this chart to get some quick information to help you differentiate between the available wireless networking standards and choose which standard might be the right fit for your business. See the links below the chart for further information on wireless networking standards.

Standard	Data Rate	Modulation Scheme	Security	Pros/Cons
IEEE 802.11	Up to 2Mbps in the 2.4GHz band	FHSS or DSSS	WEP & WPA	This specification has been extended into 802.11b.

IEEE 802.11a (Wi-Fi)	Up to 54Mbps in the 5GHz band	OFDM	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.
IEEE 802.11b (Wi-Fi)	Up to 11Mbps in the 2.4GHz band	DSSS with CCK	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 300 feet from base station. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE 802.11g (Wi-Fi)	Up to 54Mbps in the 2.4GHz band	OFDM above 20Mbps, DSSS with CCK below 20Mbps	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
Bluetooth	Up to 2Mbps in the 2.45GHz band	FHSS	PPTP, SSL or VPN	No native support for IP, so it does not support TCP/IP and wireless LAN applications well. Not originally created to support wireless LANs. Best suited for connecting PDAs, cell phones and PCs in short intervals.
HomeRF	Up to 10Mbps in the 2.4GHZ band	FHSS	Independent network IP addresses for each network. Data is sent with a 56-bit encryption algorithm.	Note: HomeRF is no longer being supported by any vendors or working groups. Intended for use in homes, not enterprises. Range is only 150 feet from base station. Relatively inexpensive to set up and maintain. Voice quality is always good because it continuously reserves a chunk of bandwidth for voice services. Responds well to interference because of frequency-hopping modulation.

HiperLAN/1 (Europe)	Up to 20Mbps in the 5GHz band	CSMA/CA	Per-session encryption and individual authentication.	Only in Europe. HiperLAN is totally ad-hoc, requiring no configuration and no central controller. Doesn't provide real isochronous services. Relatively expensive to operate and maintain. No guarantee of bandwidth.
HiperLAN/2 (Europe)	Up to 54Mbps in the 5GHz band	OFDM	Strong security features with support for individual authentication and per-session encryption keys.	Only in Europe. Designed to carry ATM cells, IP packets, Firewire packets (IEEE 1394) and digital voice (from cellular phones). Better quality of service than HiperLAN/1 and guarantees bandwidth.

Wireless Network Architecture

Access Point

An access point is the same as a 10/100 BaseT hub except that it connects using an antenna instead of wires. Wireless network cards are installed on workstations to connect to the access points. An access point almost always has at least one 10/100 BaseT port so that it can be connected to a wired network if needed. Access points can also be used to route or bridge to other access points, which allows wireless networks to extend their range.

Ad Hoc

An ad hoc network is one that doesn't use access points. It is more commonly used for smaller workgroup configurations. A small office with five computers may utilize an ad hoc configuration. In such a configuration, all workstations communicate with each other through their wireless network cards.

Securing the Wireless Network

Most access points these days have a number of security features available, but by default, they are almost always turned off. This is one of the main reasons wireless networks can be so insecure. More often than not, they are configured with default out-of-the-box settings, which mean there is no security at all. Each feature has a weakness, but by using a combination of some or all of the features, you can make a wireless network very secure—secure enough for almost any library environment. The type of wireless security features implemented can widely vary depending on the size and needs of a library. Many of the out-of-box solutions in this section are optimal for smaller libraries with limited IT staff. Please see the section on "Public Wireless Access for Enterprise Solutions" for larger scale solutions.

Default Password

After connecting to an access point for the first time, the first security consideration should be renaming the default password. Without other security features enabled, anyone could guess the default out-of-box IP address assigned to an access point and then have full administrative access to it. Not changing the default password on an access point is equivalent to leaving your front door open.

SSID/Network ID

The SSID is a 7-digit alphanumeric identifier that is set on the access point. When a client connects to an access point, it transmits a SSID to associate itself with that network. There are two modes, closed and open. In open mode, any client can connect to the access point regardless of what SSID it has. In closed mode, a client must have the correct SSID to connect. There is also a common setting that determines whether or not an access point is to advertise its SSID. By default, most access points use their company name as the SSID (i.e. "linksys" or "3COM"), are in open mode and will advertise their SSID. Therefore, to optimize maximum

security using the SSID feature, you should:

1. Change the default SSID
2. Set the SSID mode to closed
3. Set the access to not broadcast/advertise its SSID

Complying with all the above steps is not a foolproof security solution. The SSID is transmitted in clear text unless encryption is enabled (see section on encryption). It is unlikely but possible for someone with the correct knowledge and tools to reveal an SSID.

WEP (Wired Equivalency Protocol) Encryption

WEP is a protocol that encrypts data sent back and forth between the access point and a client. WEP can be enabled at two different levels: 40-bit and 128-bit. Encryption keys (passwords of a sort) can be defined on the access point. One or more keys entered on the client must match those configured on the access point in order to connect. Once connected, the data is then encrypted. This prevents someone from using a packet sniffer program to retrieve data and review its contents.

WEP has security flaws. Articles have been published outlining its weaknesses. Additionally, there are readily available tools that can crack encryption keys. Therefore, using 128-bit encryption compared to 40-bit is not necessarily important. Despite its weaknesses, WEP offers yet another line of defense from attackers breaking in to a network. Because there are so many wireless networks out there with even less security, the average hacker will more likely move on to one of those rather than spend time infiltrating one with WEP.

MAC Address Filtering

Most access points offer a feature that defines which clients may connect determined by their MAC address. A MAC address (media access layer) is a hard-coded identifying address on a network interface card that is different from an IP address. A MAC address is usually static and never changes—even when the card is removed from the computer. With MAC address filtering turned on, a workstation will not be able to connect unless its MAC address has been defined on the access point. This security feature is useful in smaller networks, although keeping a list of updated MAC addresses for a large network can be too difficult to manage.

Although the list of accepted MAC addresses is difficult, if not impossible, to extract from most access points, it is possible but unlikely for someone with the right tools and knowledge to discover one of the MAC addresses already in use on a network. An attacker could then configure a workstation to masquerade as a legitimate workstation with the "stolen" MAC address.

Control your broadcast area
Many wireless APs let you adjust the signal strength; some even let you adjust signal direction. Begin by placing your APs as far away from exterior walls and windows as possible, then play around with signal strength so you can just barely get connections near exterior walls. This isn't enough, though. Sensitive snooping equipment can pick up wireless signals from an AP at distances of several hundred feet or more. So even with optimal AP placement, the signal may leak.
Ban rogue access points

If an AP is connected to your home or office network, make sure you or the network administrator put it there. Bob in Accounting isn't likely to secure his rogue AP before he connects it. Free software like NetStumbler (www.netstumbler.com) lets you sweep for unauthorized APs.

Understanding EAP Types

Different types of EAP have been defined to support authentication methods and associated network security policies. The most widely-deployed EAP types are summarized in the following table.

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Server Authentication	None	Password Hash	Public Key (Certificate)	Public Key (Certificate)	Public Key (Certificate)
Supplicant Authentication	Password Hash	Password Hash	Public Key (Certificate or Smart Card)	CHAP, PAP, MS-CHAP(v2), EAP	Any EAP, like EAP-MS-CHAPv2 or Public Key
Dynamic Key Delivery	No	Yes	Yes	Yes	Yes
Security Risks	Identity exposed, Dictionary attack, Man-in-the-Middle (MitM) attack, Session hijacking	Identity exposed, Dictionary attack	Identity exposed	MitM attack	MitM attack

EAP-MD5 lets a RADIUS server authenticate LAN stations by verifying an MD5 hash of each user's password. This is a simple and reasonable choice for trusted Ethernets where there is low risk of outsider sniffing or active attack. However, EAP-MD5 is not suitable for public Ethernets or wireless LANs because outsiders can easily sniff station identities and password hashes, or masquerade as access points to trick stations into authenticating with them instead of the real deal.

Cisco's Lightweight EAP (LEAP) goes a notch beyond EAP-MD5 by requiring mutual authentication and delivering keys used for WLAN encryption. Mutual authentication reduces the risk of access point masquerading -- a type of Man-in-the-Middle (MitM) attack. However, station identities and passwords remain vulnerable to attackers armed with sniffers and dictionary attack tools. LEAP is mostly attractive to organizations that use Cisco access points and cards and want to modestly raise the security bar.

EAP with Transport Layer Security (EAP-TLS) is the only standard secure option for wireless LANs at this time. EAP-TLS requires the station and RADIUS server to both prove their identities via public key cryptography (i.e., digital certificates or smart cards). This exchange is secured by an encrypted TLS tunnel, making EAP-TLS very resistant to dictionary or other MitM attacks. However, the station's identity -- the name bound to the certificate -- can still be sniffed by outsiders. EAP-TLS is most attractive to large enterprises that use only Windows XP/2000/2003 with deployed certificates.

EAP with Tunneled TLS (EAP-TTLS) and **Protected EAP (PEAP)** are Internet Drafts that have been proposed to simplify 802.1X deployment. Both require certificate-based RADIUS server authentication, but support an extensible set of user authentication methods. Organizations that have not yet issued certificates to every station and don't want to just for 802.1X can use Windows logins and passwords instead. RADIUS servers that support EAP-TTLS and PEAP can check LAN access requests with Windows Domain Controllers, Active Directories, and other existing user databases. From a sniffing perspective, these options are just as strong as EAP-TLS. However, user passwords are still more likely to be guessed, shared, or disclosed through social engineering than client-side certificates.

When planning your rollout, keep in mind that EAP types like EAP-TTLS and PEAP are not yet finalized. Additional EAP types are also still being defined, including EAP-SIM (to support GSM devices with SIM cards) and EAP-SecurID (to support two-factor hardware tokens). In fact, both EAP and 802.1X are still being tweaked to overcome issues encountered by early adopters. As these solutions mature, you should anticipate the need to upgrade installed 802.1X/EAP software. To manage this cost, you may want to start with a modest 802.1X rollout. Learn the ropes and get familiar with both the benefits and challenges of 802.1X. Start improving WLAN security with 802.1X today and you'll be better prepared for company-wide deployment in the

future.

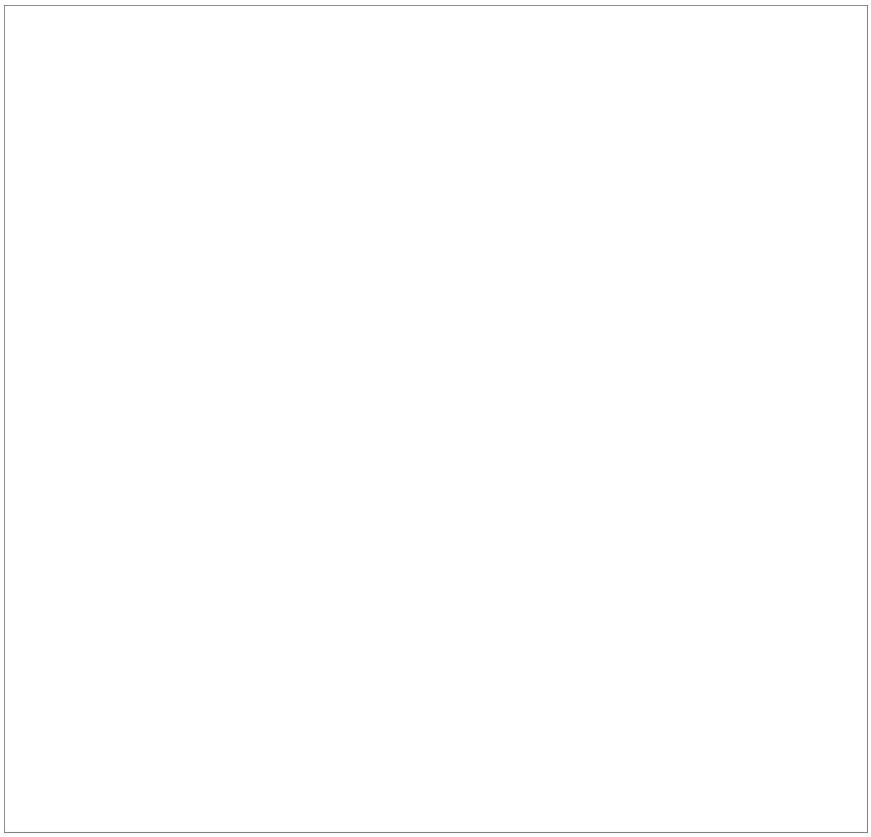
EAP Authentication

Five components are required to implement 802.1x authentication:

- **Compatible client device:** Typical clients include notebook computers and personal digital assistants (PDAs). A device that requests to join a wireless network is known as a supplicant.
- **Supplicant software:** This software provides the logic that a device needs to present its credentials and follow the proper protocol for joining the network as a client.
- **Authenticator:** The authenticator is a wireless access point that must verify the identity of a supplicant before granting the device network access.
- **Authentication server:** The authentication server is a separate system—typically running the Remote Authentication Dial-In User Service (RADIUS) or another service supporting the Extensible Authentication Protocol (EAP)—that handles authentication requests relayed by authenticators from supplicants.
- **User database:** The user database is a list of valid users and their credentials that the authentication server consults to validate authentication requests. This database may be a simple flat file or a service provided by a directory infrastructure, such as the Microsoft® Active Directory® directory service or the Lightweight Directory Access Protocol (LDAP).

The authentication process begins when a client attempts to connect to the access point, which will open a restricted port. This port allows the client to pass only EAP packets to the authentication server on the wired side of the access point. All other traffic, such as HTTP or Dynamic Host Configuration Protocol (DHCP) traffic, is blocked. The 802.1x protocol involves seven basic steps (see **Figure 1**):

1. **Request access.** The supplicant presents the authenticator with an EAP response/identity request.
2. **Limit access to authentication server.** The authenticator relays the request to the authentication server; at this point, the supplicant's access is restricted to the authentication server.
3. **Issue challenge.** The server issues a challenge and passes it back to the supplicant.
4. **Answer challenge.** The supplicant answers the challenge by sending the necessary credentials back to the authentication server.
5. **Validate response.** The server verifies the credentials against the user database; if valid, the server responds with a success message.
6. **Allow access to network.** The authenticator increases the scope of the client's access.
7. **Use other network devices.** The authenticator notifies the client that it may now participate on the network.



Consider VPNs
Most people agree that the best method of securing your wireless network is by using a combination of the suggestions above. However, the most effective strategy would be to use VPN technology. If a library has data sensitive enough to necessitate higher security than what is provided out-of-box, then VPN technology is probably the answer. To set up such a solution, access points need to be placed in the DMZ (open to the Internet) which are then connected to a VPN server. A wireless workstation connects to the VPN server using the access point and then "tunnels" into the network. The VPN client takes care of the password and data transmission encryption.

Analyzing the failure of WEP

Although WEP incorporates several mechanisms to help secure wireless traffic, many attacks have surfaced over time, demonstrating that the design goals were not achieved. Analysis of these attacks confirms that WEP fails to enforce access control, and cannot guarantee privacy or integrity of data transmissions.

Shared authentication puts access control in jeopardy
Access control to the network is most at risk when using shared authentication. Although challenging a new client to ensure it has the correct secret key may seem to enforce greater protection, this handshake provides an eavesdropper with useful information that can compromise network access.

By listening to the handshake, the eavesdropper obtains the initial unencrypted challenge message that the access point sent, as well as the encrypted message that the joining client returned. Given these two pieces of information—both plaintext and corresponding ciphertext—the eavesdropper can conduct a known plaintext attack. By forcing reuse of the compromised IV, the eavesdropper can use the known associated keystream to correctly answer the access point’s challenge. In this way, an attacker can join the network without even knowing the secret

key.

Keystream collisions compromise privacy
The authentication attack is a specific instance of a more general attack in which the privacy of any transmission can be compromised. Message privacy is at risk when any two messages are encrypted with the same keystream using a stream cipher. Because the keystream depends on a combination of the secret key and an IV, and because the secret key is constant, an eavesdropper can determine that two messages are encrypted with the same keystream—an occurrence known as a collision—simply by comparing their IVs, which are always sent unencrypted.

When an XOR operation is performed on two encrypted messages with identical IVs, the result equals the XOR result of the two messages before they were encrypted. Therefore, if parts of one unencrypted message (the plaintext) are known or can be guessed, an attacker can easily deduce corresponding parts of the other message, regardless of the size of the secret key. Given predictable message formats such as e-mail headers, some plaintext can be easily guessed. Because most wireless access points are connected to a wired network, attackers often can choose plaintext to be sent over the wireless network by sending it from a wired station—*a chosen plaintext attack*.

Such attacks would not be possible if the IV were non-repeating. However, with a 24-bit IV, at most 2^{24} (16 million) possible values exist. In high-traffic environments, IVs are guaranteed to repeat in a matter of hours. Even worse, many vendors choose to reinitialize the IV to zero every time the access point or client is started, and subsequently increment the IV for each transmitted packet. This practice means the IV is likely to be a low-value number that was recently used, resulting in even more collisions. Consider a case in which hundreds of clients, such as notebook computers, are started at nearly the same time—for example, when users arrive at work. Because they all share the same secret key, and they all start their IV counters at zero, multiple collisions are practically guaranteed. Predicting the next IV in the sequence also becomes easier, which furthers the attacker's goals.

Over time, attackers can completely compromise privacy using a *dictionary attack*. As collisions occur, attackers build a table that lists the keystream corresponding to each IV. Once every IV value has been observed in collision, all transmissions are compromised.

Checksum and keystream weaknesses invite attacks on data integrity
CRC-32's linearity and independence from the secret key and IV can compromise data integrity. CRCs are designed to detect random errors, not malicious or intentional modifications. The receiver accepts the message after decryption if the checksum appended to the message matches the checksum computed on the received data. Because CRC-32 is a linear function, the checksum of a message can easily be modified to pass inspection. If an attacker modifies a data packet, and changes the appended checksum to reflect this modification, the receiver will unknowingly accept the message as unaltered.

Attackers also can compromise data transfer integrity by injecting a new message into the network. Again, by knowing a message in unencrypted and encrypted forms, attackers can determine the keystream. Using this keystream and the corresponding IV, attackers can inject a new message with the correctly calculated checksum into the network. The receiver simply verifies that the checksum is correct and accepts the message. Note that in all these attacks the eavesdropper is never required to know the secret key, and that the length of the key is irrelevant.

The Future

Although nearing completion, the 802.11i standard is still some time away from reaching the market. Wireless vendors have released key components of 802.11i technology now, under the name Wireless-Fidelity, or Wi-Fi, Protected Access. WPA has the following features:

- Backward compatibility with 802.11 hardware
- Software or firmware upgrade
- 802.1x
- TKIP

- Michael algorithm
- Key management and key hierarchy

Some 802.11i features do not appear in WPA because they require a hardware upgrade. Other 802.11i features are not perceived as urgent, or are not yet sufficiently specified:

- **AES:** Implementing this feature would require a hardware upgrade, because the encryption and decryption functions cannot be performed quickly enough in software.
- **CCMP and WRAP:** The Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and Wireless Robust Authenticated Protocol (WRAP) are AES-based replacements for TKIP. Whereas TKIP is an evolution of WEP, CCMP and WRAP have been designed exclusively for 802.11i and offer improved security. Because these protocols are AES-based, they require a hardware upgrade.
- **IBSS:** 802.11i will address independent basic service sets (IBSSs), also known as ad hoc or peer-to-peer wireless networks. WPA instead focuses on extended service sets (ESSs), which are networks formed around wireless access points. An IBSS has no access point; an ESS has multiple access points.
- **Preauthentication:** For applications that require minimal latency, such as voice over IP (VoIP), 802.11i will provide preauthentication as a way to reduce latency during hand-off between basic service sets (BSSs). A BSS is a network of wireless devices sharing the same access point. Preauthentication will essentially reduce the time necessary for communication to resume when a client moves between access points. This feature is not perceived as urgent.

The figure below shows the expected progression of wireless security technology. The original combination of 802.11 and WEP has already been successfully augmented by the 802.1x authentication protocol. The introduction of WPA by the Wi-Fi Alliance makes the most important features of 802.11i available now, requiring only software upgrades. When 802.11i is ready, it will be marketed as WPA-2, offering forward compatibility with WPA. Through hardware upgrades additional features will become available, such as the stronger AES cipher and improved security protocols using AES, IBSS support, and preauthentication support. As security standards for wireless networking improve, business and government organizations may feel more confident about adopting this technology—giving them the opportunity to reap its productivity benefits.