Secure Wi-Fi Technologies for Enterprise LAN Network

Tom Borick
Rivier College
CS575A Advanced Local Area Networks (LANs)
Dr. Vladimir V. Riabov

Secure Wi-Fi Technologies for Enterprise LAN Network
Tuesday, April 26, 2005

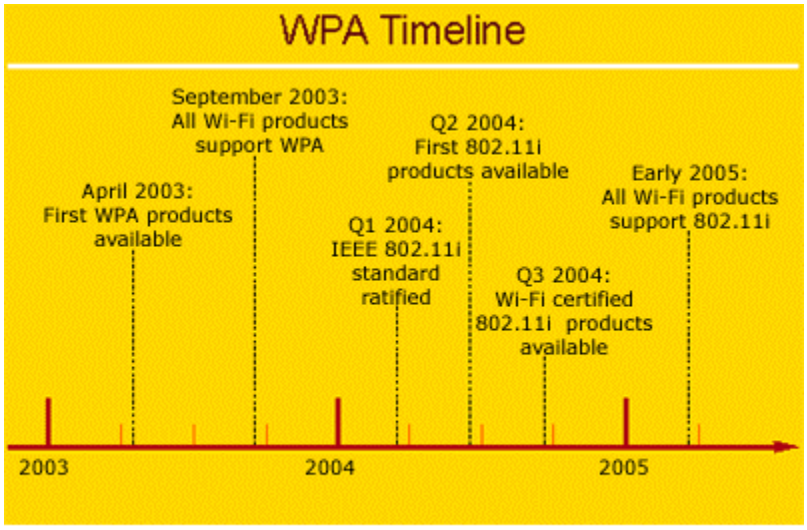
Table of Contents

Executive Summary

Secure Wi-Fi technologies for enterprise local area networks are desirable to the enterprise because they provide a secure access to the enterprise network without having to install cables for connectivity. Wi-Fi technology can be designed to meet the needs of a mobile workforce. However, additional assessment of enterprise needs and LAN infrastructure are needed to ensure enterprise-class security.

To address enterprise network security, IEEE introduced the Wired Equivalent Privacy (WEP). This optional security measure was meant to secure 802.11b /9/wi-Fi) WLANs, but inherent weaknesses in the standard have been identified.

This paper will review the Wi-Fi connection, Wi-Fi Technology, designing the Wi-Fi network, Wi-Fi Security, Wi-Fi Terms, Wi-Fi Resources and a conclusion on the recommendation to add secure Wi-Fi technologies to the enterprise-class secure local area network.



Slow But Secure. Though 802.11i was originally planned for 2002, products will not be available until mid-2004 at the earliest. (7)

Introduction

Wi-Fi Technology

Wi-Fi networks use radio technologies called IEEE 802 11b or 80211a to provide secure, reliable, fast wireless connectivity to existing networks. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wired enterprise local area networks (which use IEEE 802.3 or Ethernet). Wi-Fi networks operate in the unlicensed 2.4 and 5 GHz radio bands, with an 11 Mbps (802.11b) or 54 Mbps (802.11a) data rate or with products that contain both bands (dual band), so they can provide real-world performance similar to the basic 10BaseT wired Ethernet networks used in enterprise-

secure local area networks. Wi-Fi LAN Technology is categorized by transmission type and physical media. Wi-Fi Technology fall into one of the following four categories [5]:

- **Infrared LANs** at 1 Mbps and 2 Mbps operates at a wavelength between 850 and 950 nm. An individual cell of an IR LAN is limited to a single room because infrared light does not penetrate opaque walls.
- **Direct-sequence spread spectrum** operates in the 2.4 GHz ISM band. Up to seven channels, each with a data rate of 1 Mbps and 2 Mbps can be used. In most cases, these LANs operate in the ISM (industrial, scientific, and medical) bands so that no FCC licensing is required for use in the United States. Under Direct-sequence each bit in the original signal is represented by multiple bits in the transmitted signal, know as a chipping code. The chipping code spreads the signal across a wider frequency band in direct proportion to the bits used. Therefore a 10-bit chipping code spreads the signal across a frequency band that is 10 times greater than the 1-bit chipping code.
- **Frequency-hopping spread spectrum** operates in the 2.4 GHz ISM band, at data rates of 1 Mbps and 2 Mbps. In most cases, these LANs operate in the ISM (industrial, scientific, and medical) bands so that no FCC licensing is required for use in the United States. Under Frequency-hopping the signal is broadcast over seemingly random series of radio frequencies, hopping from frequency to frequency at fixed intervals. A receiver, hopping between frequencies in synchronization with the transmitter, picks up the message. Would-be eavesdroppers hear only unintelligible blips. Attempts to jam the signal succeed only in knocking out a few bits.
- **Narrowband microwave LANs** operate at microwave frequencies but do not use spread spectrum.

Wi-Fi Mobility Stations

IEEE802.11 defines three types of stations based on mobility [5]:

- No transmission: A station either stationary or moves only within the direct communications range of the communicating stations of a single Basic Service Set (BSS).
- BSS transmission: This is defined as a station movement from one BSS to another BSS within the same Extended Service Set (ESS). Delivery of data to the station requires that the addressing capability be able to recognize the new location of the station.
- ESS transition: This is defined as a station movement from a BSS in one ESS to a BSS within another ESS. This case is supported only in the sense that the station can move. Maintenance of upper-layer connections supported by 802.11 cannot be guaranteed. Disruption of service is likely to occur.

Wi-Fi IEEE802.11 Services

There are five types of services for Wi-Fi IEEE802.11 [5]:

- Association: Establishes an initial association between a station and an access point within a particular BSS. The access point can then communicate

information (station identity, its address) to other access points within the ESS to facilitate routing and delivery of addressed frames.

- Reassociation: Enables an established association to be transferred from one access point to another, allowing a mobile station to move from one BSS to another.
- Disassociation: A notification from either a station or an access point that an existing association is terminated.
- Authentication: Used to establish the identity of stations to each other. The standard does not mandate any particular authentication scheme, which could range from insecure handshaking to public-key encryption schemes.
- Privacy: Used to prevent the contents of message from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy.

Medium Access Control

IEEE802.11 provides a Medium Access Control (MAC) algorithm called DFWMAC (distributed foundation wireless MAC) that provides a distributed access control mechanism with an optional centralized control on top of that for Wi-Fi [5]. The lower sublayer of the MAC layer is the distributed coordination function (DCF). The DCF sublayer makes use of a simple CSMA contention algorithm to provide access to all traffic. If a station has a MAC frame to transmit, it listens to the medium. If the medium is idle, the station may transmit: otherwise the station must wait until the current transmission is complete before transmitting. The DCF does not include a collision detection function because collision detection is not practical on a wireless network.

Wi-Fi Multimedia

WMM stands for Wi-Fi Multimedia, features that improve the user experience for audio, video and voice applications over a Wi-Fi® network [14]. WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. “The demand for Wi-Fi CE product connectivity is expected to grow significantly and WMM will provide a strong foundation for that growth. In fact, we see this action jumpstarting the coming mainstream adoption of Wi-Fi in the consumer electronics market segment,” said Wi-Fi Alliance Managing Director, Frank Hanzlik. “The Alliance’s WMM certification testing will help unleash a new category of wireless products that use the robust connectivity only offered by Wi-Fi CERTIFIED interoperability. The demand for multimedia support in telephony and other consumer electronic products has skyrocketed in the recent months and is forecasted to grow at an unprecedented rate,” Hanzlik added, **The Wi-Fi Alliance Press Release, September 8, 2004.** To meet this need the Wife Alliance started interoperability certification for WMM as a profile of the IEEE802.11e QoS (Quality of Service) extensions for 802.11 networks [14]. The following Wi-Fi CERTIFIED products are the first to have obtained WMM certification **The Wi-Fi Alliance Press Release, September 8, 2004**.

Atheros Communications Inc.
- Atheros AR5002AP-2X Concurrent 802.11a and 802.11b/g Dual-band Access Point
- Atheros AR5002X Universal 802.11a/b/g Wireless Network Adapter

Broadcom Corporation
- Broadcom AirForce™ 802.11a/g CardBus Reference Design, BCM94309CB
- Broadcom AirForce™ 802.11a/g Access Point Reference Design, BCM94704-AGR

Cisco Systems
- Cisco Aironet 1200 Series Access Point with integrated 802.11a and 802.11g radios

Conexant Systems, Inc.
- ISL39200C WorldRadio

Instant802 Networks
- Gateway 7001 Access Point

Intel
- Intel® Pro/Wireless 2915 Network Connection

Philips
- Philips 802.11 a/g WLAN Reference Design SA5250/1 mPCI

What is Enterprise-Level Wi-Fi

Enterprise-Level Wi-Fi technology connects the enterprise network to anywhere in the world. This includes using a Wi-Fi network to connect multiple computers to each other, to peripherals, and to the enterprise with an Internet interface. A Wi-Fi network can connect enterprise computers together to share such hardware and software resources as printers and the Internet. That means everyone in the enterprise can share stored files, photos and documents and print them out on a single printer attached to one desktop computer—all without expensive cables running throughout the enterprise. In a home office, Wi-Fi CERTIFIED equipment in a wireless network provides the ability to share a single high-speed broadband cable or DSL connection interface to the enterprise network. A small remote CERTIFIED Wi-Fi network can expanded to ten users and work with the equipment added to the future network. Wi-Fi networks also work well for the mobile work force, providing connectivity between mobile salespeople, floor staff and behind-the-scenes finance and accounting departments. Because mobile workforce departments are dynamic, the built-in flexibility of a Wi-Fi network makes it easy and affordable for them to change and grow.

What is Enterprise Local Area Network Connectivity Problem?

Large corporations and campuses use enterprise-level technology and Wi-Fi CERTIFIED wireless products to extend standard wired Ethernet networks to public areas like meeting rooms, training classrooms and large auditoriums. Many corporations also provide wireless networks to their off-site and telecommuting workers to use at home or in remote offices. Large companies and campuses often use Wi-Fi to connect buildings. Service providers and wireless ISPs are using Wi-Fi technology to distribute Internet connectivity within individual homes and businesses as well as apartments and commercial complexes. The problem is providing a secure interface for a mobile workforce to the enterprise local area network.

Mobile Connectivity

Wi-Fi networks are also found in busy public places like coffee shops, hotels, airport lounges and other locations where large crowds gather. This may be the fastest-growing segment of Wi-Fi service, as more and more travelers and mobile professionals clamor for fast and secure Internet access wherever they are. Soon Wi-Fi networks will be found in urban areas providing coverage throughout the central city, or even lining major highways, enabling traveler's access anywhere they can pull over and stop.

LAN vs. Wi-Fi LAN

Wireless computers can be added to a Wi-Fi network without the LAN requirement to lay cable or find an available Ethernet port on a hub or router. Wi-Fi LAN network connectivity is completed with a plug in card or USB connection on the computer. When employees move the enterprise does not have to abandon the network infrastructure investment or hire a networking company to rewire the new location. There's no required network downtime to plug the system into a new power outlet and be operational in minutes.

Designing the Wi-Fi Network

What Makes Up a Wireless Network?

Wi-Fi devices "connect" to each other by transmitting and receiving signals on a specific frequency of the radio band. Components can connect to each other directly (this is called "peer-to-peer") or through a gateway or access point. Wi-Fi networks consist of two basic components: Wi-Fi radios and access points or gateways. Wi-Fi radios are embedded or attached to the desktop computers, laptops and mobile devices in your network. The access points or gateways act as "base stations" — they send and receive signals from the Wi-Fi radios to connect the various components to each other as well as to the Internet. All computers in your Wi-Fi network can then share resources, exchange files and use a single Internet connection.

Peer-to-Peer Network or an Access Point or Gateway

A peer-to-peer network is composed of several Wi-Fi equipped computers talking to each other without using a base station (an access point or gateway). All Wi-Fi CERTIFIED™ equipment supports this type of wireless set-up, which can be useful for transferring data between computers or sharing an Internet connection among a few computers in a room. A peer-to-peer wireless network can be a less expensive solution for three or fewer computers, but most enterprises use an access point to connect Wi-Fi devices since this will provide for the best performance and allow for easier Internet sharing.

Wi-Fi Radio Options for Laptops, Desktops and PDAs

Many laptop computers and mobile computing devices come with a Wi-Fi radio built in. They're ready to operate wirelessly. Laptops without a built in radio require a Wi-Fi radio

embedded in a simple PCMCIA (Personal Computer Memory Card International Association) card to be installed in the laptop's expansion slot. There are several ways to include desktop computers in the enterprise network. Since most don't provide slots for PC Cards, the simplest method is to use a USB (Universal Serial Bus) Wi-Fi radio that plugs into an available USB port on your desktop computer. Computers without a USB port require the installation of a PCI or ISA bus solution. This requires removal of the desktop casing to find an available PCI or ISA bus slot. The manufacturer's set-up instructions will describe installation of the device. (Some Wi-Fi manufacturers provide one-piece ISA and PCI bus radios. Others provide ISA or PCI bus adapters that enable you to use the same slide-in Wi-Fi PC Cards that you would use in your laptop.) Apple offers an embedded Wi-Fi radio, the Apple AirPort Radio, which can be installed in new Macintosh computers. Personal Digital Assistants like Palm™, Visor™ and Pocket PC™ have a slot for a Compact Flash format Wi-Fi radio. (Some laptops also have Compact Flash capability.) There are also new small-format Wi-Fi radios for PDAs and mobile data devices becoming available, offering additional options for wireless connections in the future.

Planning for Access Points and Gateways

The Wi-Fi access point or gateway functions as the base station for the network. This is the central connection among all wireless client devices, laptop computers, PDAs, desktop computers and wireless peripherals like printers. The base station sends and receives radio signals to and from the Wi-Fi radio in the laptop or PC, enabling the sharing of the Internet connection with other users on the network. Access points and gateways have a wide range of features and performance capabilities, but they all provide this basic network connection service.

How Many Users Can Use a Single Access Point?

Wi-Fi networks, like wired networks, are a shared medium. An 802.11b Wi-Fi network may provide 11 Mbps of bandwidth to an individual user. Theoretically, if ten users are simultaneously using the network, each will have to share and may only get 1 Mbps or so each. However, network sharing is not quite this simple. A lot depends on the users' behaviors. Someone who is just sending and receiving e-mail just uses the wireless connection in bursts. They will probably never notice any slow down. On the other hand, a roomful of Wi-Fi users who are accessing high-resolution multimedia over a single access point may indeed notice a slowdown. In this instance, they may require additional access points or higher speed access points that use 802.11a or 802.11g that provide 54 Mbps or better of bandwidth. Depending on how the users connect and what they do once they are on the network, you may need to use higher speed access points, as well as more of them.

Choosing Components for the Wi-Fi Network

To set up a Wi-Fi network, you need to consider the components, the users and how you will use the network. Each component will need a Wi-Fi radio. Laptops not preconfigured with an embedded Wi-Fi radio need a Wi-Fi PC Card radio. Each desktop will need either a Wi-Fi USB adapter (which combines a PC Card radio with a USB converter circuit) or a Wi-Fi PCI/ISA adapter (which is a radio available with or without

a built-in PC Card reader). Desktop computers with sufficient USB jacks for a USB adapter hookup require Windows™ 98 or newer. PDAs will also need radio devices. Some can use the same PC Card used in laptops; some use Compact Flash. Wi-Fi access points or gateways serve as the central base station for your network. A typical Wi-Fi access point can support some 15 to 20 users within100 to 300 feet indoors and 2000 feet outdoors. The range may vary, based on the building or environment. The number of access points depends on how the network is used and the total number of users, as well as how big a space needs to be covered. A single access point can easily handle from 10 to 30 users who only use the network to send e-mail, cruise the Internet and occasionally save and retrieve large files. Within a typical office environment, most access points can provide good wireless coverage up to 150 feet or so. Large facilities with many users, or with users who require a lot of bandwidth, need more than a single access point. Many access points can be connected to each other wirelessly or via Ethernet cables to create a single large network.

Printers on a Wi-Fi Network

To share printers, connect them to a computer on the network, dedicate a Wi-Fi equipped computer to act as a printer server, or connect a Wi-Fi equipped printer or print server to the network to control your print jobs. (A shared printer connected to a computer must have the computer turned on to access the printer via the wireless Wi-Fi connection.)
A wireless print server is a small computer and Wi-Fi radio built into a single box; a Wi-Fi equipped printer connects directly to the Wi-Fi network. A Wi-Fi print server or a Wi-Fi equipped printer can make a printer accessible to the enterprise network.
Many additional Wi-Fi enabled devices will soon be appearing. Each will have its own embedded Wi-Fi radio to connect directly to the enterprise network. The devices won't need to connect enterprise Wi-Fi peripherals to an always-on computer or a stand-alone Wi-Fi radio adapter. These devices can include scanners, cameras, telephony devices, video and TV monitors, DVD players, appliance controllers, multimedia players and recorders.

Sharing Devices on the Network

If you don't need to have each computer on the network all the time, you can save money by sharing the PC Cards for your laptops and other mobile computing devices and the USB radio/adapters for your PCs and laptops. For example, when you're working in the office, your USB radio can be connected to your desktop computer. When you go on the road with your laptop, the same USB device can connect to your laptop computer's USB slot to provide mobile connectivity. When you're at home, you can hook the same USB radio to your desktop computer and use it to access your home Wi-Fi network.

Security Technologies

WPA and other wireless encryption methods operate strictly between a Wi-Fi enabled computer and the enterprise Wi-Fi CERTIFIED™ access point. When data reaches the access point or gateway, it is unencrypted and unprotected while it is being transmitted out on the public Internet to its destination — unless it is also encrypted at the source

with SSL when purchasing on the Internet or when using a VPN. So while using WPA will protect the enterprise from external intruders, enterprises can also implement additional techniques to protect enterprise secure network transmissions when using public networks and the Internet. There are several technologies available, but currently VPN works best

Wi-Fi Protected Access for Enterprise Security Needs

Wi-Fi Protected Access 2™ (WPA2) builds on its predecessor, WPA™, and is specifically designed to meet enterprise-secure network needs. WPA2 is based upon the Institute for Electrical and Electronics Engineers' (IEEE) 802.11i amendment. *Many enterprise organizations have been seeking an interoperable, Wi-Fi CERTIFIED technology based on the full IEEE 802.11i standard. Others require AES encryption for internal or regulatory reasons. WPA2 meets these needs. Furthermore, because WPA2 is backwards- compatible with WPA, organizations that have already implemented the WPA standard can migrate to WPA2 at their own pace. Enterprise security needs are not a stationary target and the Wi-Fi Alliance is committed to certification programs that meet evolving security requirements. WPA2 is ideally suited for enterprises in both the public and private sectors. Products that are CERTIFIED for WPA2 give IT managers the assurance that the technology meets interoperability standards and in turn, helps them manage support and deployment costs (the 802.11 standard was ratified on July 29, 2004). The primary difference between WPA and WPA2 is that WPA2 uses a more advanced encryption technique called AES (Advanced Encryption Standard), allowing for compliance with FIPS140-2 government security requirements. Products that are Wi-Fi CERTIFIED for WPA remain technically sound and secure.* (6)

Wireless LAN Security Standards

	WEP	WPA	802.11i (RSN, WPA2)
Cipher Algorithm	RC4	RC4 (TKIP)	Rijndael (AES-CCMP)
Encryption Key	40-bit	128-bit (TKIP)	128-bit (CCMP)
Initialization Vector	24-bit	48-bit (TKIP)	48-bit (CCMP)
Authentication Key	None	64-bit (TKIP)	128-bit (CCMP)
Integrity Check	CRC-32	Michael (TKIP)	CCM
Key Distribution	Manual	802.1x (EAP)	802.1x (EAP)
Key unique to:	Network	Packet, session, user	Packet, session, user
Key hierarchy	No	Derived from 802.1x	Derived from 802.1x
Cipher Negotiation	No	Yes	Yes
Ad-hoc (P2P) security	No	No	Yes (IBSS)
Pre-authentication (wired LAN)	No	No	Using 802.1x (EAPOL)

Compromised Security. WPA fixes all the known holes in WEP, but it doesn't include all the advanced features of IEEE 802.11i.

(7)

Products with WPA2 Wi-Fi Security Certification

Atheros Communications Inc.
- Atheros AR5002AP-2X Concurrent 802.11a and 802.11b/g Dual-band Access Point
- Atheros AR5002X Universal 802.11a/b/g Wireless Network Adapter

Broadcom Corporation
- Broadcom AirForce™ 802.11a/g CardBus Reference Design, BCM94309CB
- Broadcom AirForce™ 802.11a/g Access Point Reference Design, BCM94704-AGR

Cisco Systems
- Cisco Aironet 1200 Series Access Point with integrated 802.11a and 802.11g radios

Instant802 Networks
- Gateway 7001 Access Point

Intel
- Intel® Pro/Wireless 2915 Network Connection

Realtek
- Realtek RTL8185&8255 802.11a/g 54M WLAN NIC / RTL8185&8255-NIC

Wi-Fi Interference

Cordless telephones, wireless microphones, and amateur radio operate at around 900 MHz cannot interfere with Wi-Fi™ equipment. Devices like a microwave oven that operate at 2.4 GHz have greater leakage of radiation with increasing age [13].

A special multicarrier modulation method (OFDM) is used for dividing the 5.8-GHz band into 52 subbands for sending 48 groups of bits at a time and 4 subbands for control information by one source at a given time [16]. Dividing the band into subbands diminishes the effects of interference. As a result, only few unlicensed narrowband microwave-radio-frequency devices (e.g., RadioLAN™ equipment) can slightly interfere with the Wi-Fi™ equipment operating at 5.8 GHz.

The new IEEE 802.11g specification also uses the OFDM modulation method with a 2.4-GHz band that significantly reduces the effects of interference (e.g., with the old microwave oven). In addition, if the subbands are used randomly, security can be increased.

Cracking Wi-Fi Protected Access

We have reviewed products with WPA2 Wi-Fi security certification; we will now look at research done to investigate how WPA can be cracked. Let's illustrate how WPA can be cracked using a program written by Joshua Wright, in an article written by Seth Fogie, Cracking Wi-Fi Protected Access, 3/11/2005 [18]. Wright's research prompted Cisco to release a warning about the insecurities of LEAP that eventually lead to the release of EAP-Fast. Mr. Wright also produced the first publicly available WPA cracking tool for Linux. While KisMAC had this ability for several months prior to the release of

coWPAtty, the use of that tool requires a Mac. Mr. Wright's article showed how you can use coWPAtty to crack WPA. You can find coWPAtty in a bootable Linux project called Auditor (under the guise of wpa-psk-bf) and online at SourceForge. WPA will be cracked by coWPAtty by testing numerous passwords, in order, one at a time, 30–60 words per second. You need to provide a password list, a capture file with a complete EAP four-way handshake, as well as the SSID for the target network. The following sections outline the steps to collect the handshake and SSID.

Collecting Data

Prior to using coWPAtty, Wright captured a WPA-PSK TKIP/EAP/802.1x negotiation session between an access point and a node. This can be accomplished using any number of sniffers, including Ethereal and tcpdump.

The illustration is a highly filtered capture of only four packets, each of which represents one of the parts of the four-way handshake. In a normal capture, you would see WLAN management packets and encrypted traffic from other connected devices. You must have all four packets associated with the handshake. The problem is how to differentiate one EAP packet from another.

Fortunately, the 802.11 specifications help. Figures 1-4 provide the details of each individual packet in Ethereal. Note that the ACK flag is set only when the packet originates from the Linksys AP. Also, note the encryption information that appears only in packets 2 and 3. Finally, the Install flag is set only in packet 3, which comes from the authenticator.

Figure 1 Packet 1.

Figure 2 Packet 2.

Figure 3 Packet 3.

Figure 4 Packet 4.

Joshua Wright's tool takes all these differences into consideration and automatically determines whether a packet capture contains the relevant data required to crack WPA. If any one of these packets is missing, cracking efforts will fail.

Finding the SSID

The SSID is needed to convert the PSK into a PMK in the cracking process. Most wireless client programs include a rudimentary scanner that can detect open wireless networks with detail about the type of encryption and signal strength. However, if the wireless network is not broadcasting is SSID, you'll need to do one of three things:

- "Social engineer" the SSID from a user.
- Use Kismet to monitor the traffic to pick-up the SSID the next time a user sends out a probe for the network.
- Use a program such as such as void11, wlan_jack, or essid_jack to disconnect the user from the network. If disconnected, a wireless device automatically attempts to re-authenticate, which causes the SSID to be sent over the air in plaintext.

coWPAtty Password Cracker

Seth Fogie, Cracking the Wi-Fi Protected Access, identifies the weakness of WPA is the calculated MIC value that is used to validate messages 2–4 of the four-way handshake because, coWPAtty targets the final EAPoL message. The MIC value is created by passing the entire EAPoL message into an HMAC_MD5 hashing algorithm, which is secured by the MIC Key that was taken from the PTK.

Because both the MIC value and the EAPoL message are passed as plaintext, an attacker can focus on the MIC hash value. The challenge is tied to the fact that an attacker must first convert the dictionary word to a PMK, using the correct algorithm with an accurate SSID value. Then the resulting value is plugged into another equation that also requires the MAC addresses and Nonce values of the supplicant and authenticator. The result of this calculation is the PTK, from which the attacker can strip the MIC Key. With this MIC Key, the attacker then performs the same HMAC_MD5 hash on the captured EAPoL message to see whether the selected password produces the same MIC as the captured MIC.

The WPA Wi-Fi Cracking Process

Seth Fogie, Cracking the Wi-Fi Protected Access, added a few output commands to coWPAtty to show how the program is collecting and manipulating data to produce its calculated MIC value. Nothing was altered that changes the way in which the program functions.

1. Verification of capture. This part of the program verifies that all the required packets are in the capture file. This objective is accomplished by filtering out all packets that don't include the 802.1x Authentication type flag (0x888E). The remaining packets are then checked to be sure that a complete four-way handshake was captured.
2. The packets are parsed for all relevant information. The following example lists important parts to be used during the cracking process. Figures are taken from previous Ethereal capture images.
    - Packet 1 (A>S): Provides no real data for the cracking process.
    - Packet 2 (S>A): Provides the SNonce value (green) shown in Figure 5.

      Figure 5 Packet 2 with SNonce value highlighted.

    - Packet 3 (A>S): Provides the ANonce value (green) and the MAC addresses of both the Authenticator (blue) and Supplicant (red). The MAC addresses could be taken from any one of these packets (see Figure 6).

      Figure 6 Packet 3 with ANonce value and MAC addresses highlighted.

    - Packet 4: (S>A): Provides the MIC value and EAPoL packet to be used when calculating the test MIC from the generated MIC Key (see Figure 7). Note that the MIC value is added after it's calculated. Until it's added, the data field is filled with 00 bytes.

Figure 7 Packet 4 with EAP frame data and MIC value highlighted.

3. The selected test password is checked to be sure that it's not less than eight or greater than 63 characters, as required by 802.11i.
4. The PMK is generated from the test password, using the following algorithm:
5. PMK = pdkdf2_SHA1(passphrase, SSID, SSID length, 4096)
PMK = pbkdf2_sha1("radiustest","linksys54gh",11,4096)

6. The PTKs are generated from the PMK, using the following algorithm:
7. = PRF-X(PMK,
8. Len(PMK), "Pairwise key expansion",
9. Min(AA,SA) || Max(AA,SA) || Min(ANonce,SNonce) || Max(ANonce,SNonce))
10.
11. PTK = SHA1_PRF(
12. 9e99 88bd e2cb a743 95c0 289f fda0 7bc4 ;PMK
13. 1ffa 889a 3309 237a 2240 c934 bcdc 7ddb
14. ,32,"Pairwise key expansion", ;length of PMK & string
15. 000c 41d2 94fb 000d 3a26 10fb 893e e551 ;MAC and nonce values
16. 2145 57ff f3c0 76ac 9779 15a2 0607 2703
17. 8e9b ea9b 6619 a5ba b40f 89c1 dabd c104
18. d457 411a ee33 8c00 fa8a 1f32 abfc 6cfb
19. 7943 60ad ce3a fb5d 159a 51f6,76)
20.
21. PTK = ccbf 97a8 2b5c 51a4 4325 a77e 9bc5 7050
22. daec 5438 430f 00eb 893d 84d8 b4b4 b5e8
23. 19f4 dce0 cc5f 2166 e94f db3e af68 eb76
80f4 e264 6e6d 9e36 260d 89ff bf24 ee7e

24. A MIC value is calculated, using the MIC Key from the PTK and the EAPoL message:
25. MIC = HMAC_MD5(MIC Key,
26. 16,
27. 802.1x data)
28.
29. MIC = HMAC_MD5(
30. ccbf 97a8 2b5c 51a4 4325 a77e 9bc5 7050 ;first 16 bytes of PTK
31. ,16, ;length of PTK
32. 0103 005f fe01 0900 0000 0000 0000 0000 ;802.1x data
33. 1400 0000 0000 0000 0000 0000 0000 0000
34. 0000 0000 0000 0000 0000 0000 0000 0000
35. 0000 0000 0000 0000 0000 0000 0000 0000
36. 0000 0000 0000 0000 0000 0000 0000 0000
37. 0000 0000 0000 0000 0000 0000 0000 0000

38. 0000)
MIC = d0ca 4f2a 783c 4345 b0c0 0a12 ecc1 5f77

39. The calculated MIC is compared to the captured MIC:
40. Calculated MIC using EAP frame four with "radiustest" is
41. d0ca 4f2a 783c 4345 b0c0 0a12 ecc1 5f77
42.
43. Capture MIC is
44. d0ca 4f2a 783c 4345 b0c0 0a12 ecc1 5f77
45.
CALCULATED MICS MATCH!!! Congratulations, the PSK is "radiustest".

Cracking WPA Summary

When WPA-PSK is setup with a weak password the wireless network is still exposed to attackers. However cracking the password is not easy. The attacker must have an insider's understanding of how the packets are created and how their data is used to secure a WPA-PSK network. Seth Fogie, Cracking Wi-Fi Protected Access, 3/11/05, provided an example to expose a random network, from an attacker with a large dictionary file, a powerful computer, and a little luck in order to obtain the password.

Future Wi-Fi Development Issues

MS Windows™, Mac OS™, Unix™ and Linux™ using Wi-Fi-certified equipment may have communication compatibility issues over spread spectrum (2.4-GHz and 5.8-GHz bands). The client hardware is typically a PC card or a PCI card, although USB and other forms of Wi-Fi radios are also being introduced [15]. Future speed improvements are expected in both the 2.4 and 5.8 GHz bands. Several amendments (802.11e, h, i, and n, among others) to the IEEE 802.11 standard address quality of service, adaptive signal use, security, and higher throughput [15]. According to Parks Associates, demand for CE connectivity is expected to increase by the factor of 5 by year 2007, and reach $150B. A new type of Wi-Fi products [based on the IEEE 802.11e Quality-of-Service standard and known as Wi-Fi Multimedia (WMM™)] is currently introduced to consumers [15]. The WMM™ products improve user experience for audio, video and voice applications over a Wi-Fi™ network. The WMM technology prioritizes streams of "content" and optimizes the way the wireless network allocates bandwidth among competing applications (e.g., with WMM, video transmission can have priority over data transfer).

Conclusion

In conclusion Secure Wi-Fi technologies for enterprise local area networks are desirable to the enterprise because they provide a secure access to the enterprise network without having to install cables for connectivity. Wi-Fi technology can be designed to meet the needs of a mobile workforce. However additional assessment of enterprise needs and LAN infrastructure are needed to ensure enterprise-class security.To address enterprise network security IEEE introduced the Wired Equivalent Privacy (WEP). This optional security measure was meant to secure 802.11b /9/wi-Fi) WLANs, but inherent weaknesses in the standard have been identified. In response the Wi-Fi Alliance announced new security architecture in September 2004 that addresses the short comings of WEP. This standard, formally know as Safe Secure Network (SSN), is designed to work with existing 802.11 products and offers forward compatibility with 802.11i, the new wireless security architecture defined by IEEE. WPA offers the following benefits: enhanced data privacy, robust key management, data origin authentication, and data integrity protection. WPA, the new tunneled EAP methods and the natural maturing of 802.1X should result in more robust adoption of WLAN technology for enterprise-class security. WPA works with existing 802.11 based hardware, although firmware upgrades are required, and offers forward compatibility with 802.11i.

Glossary

10BaseT

The most common cabling method for Ethernet. 10BaseT conforms to IEEE standard 802.3. It was developed to enable data communications over unshielded twisted pair (telephone) wiring at speeds of up to 10 megabits per second up to distances of approximately 330 feet on a network segment. (See Ethernet).

3G

The term refers to digital, packet-switched technology and is used to describe the third-generation of mobile telephony which brings video and broadband Internet access to mobile phones. The first generation was represented by analog cellular phones and the second generation by digital cellular networks.

802.11

A group of wireless networking standards, also known as Wi-Fi, set by the Institute of Electrical and Electronics Engineers (IEEE). (See IEEE).

802.11a

An IEEE standard for a wireless network that operates at 5 GHz with rates up to 54Mbps.

802.11b

An IEEE standard for a wireless network that operates at 2.4 GHz with rates up to 11Mbps.

802.11d

An IEEE specification that allows for configuration changes at the Media Access Control layer (MAC layer) level to comply with the rules of the country in which the network is to be used. (See MAC).

802.11e

An IEEE standard that adds Quality of Service (QoS) features and multimedia support to the existing 802.11b, 802.11g, and 802.11a wireless networks. (See QoS, WMM).

802.11g

An IEEE standard for a wireless network that operates at 2.4 GHz Wi-Fi with rates up to

54Mbps.

802.11i

An IEEE standard specifying security mechanisms for 802.11 networks. 802.11i makes use of the Advanced Encryption Standard (AES) block cipher. The standard also includes improvements in key management, user authentication through 802.1X and data integrity of headers. (See 802.1X, AES, WPA2).

802.11j

An IEEE specification for wireless networks that incorporates Japanese regulatory requirements concerning wireless transmitter output power, operational modes, channel arrangements and spurious emission levels.

802.11n

A taskgroup of the IEEE 802.11 committee whose goal is to define a standard for high throughput speeds of at least 100Mbps on wireless networks. The standard is expected to be ratified by 2007. Some proposals being fielded by the taskgroup include designs for up to 540 Mbps. Multiple-Input-Multiple-Output (MIMO) technology, using multiple receivers and multiple transmitters in both the client and access point to achieve improved performance is expected to form the basis of the final specification. (See Mbps, MIMO).

802.1X

A standard for port-based authentication, first used in wired networks, that was adapted for use in enterprise WLANs to address security flaws in WEP, the original security specification for 802.11 networks. 802.1X provides a framework for authenticating users and controlling their access to a protected network and dynamic encryption keys to protect data privacy. (See EAP, WEP, WPA, WPA2).

802.3

The standard defining wired Ethernet networks. (See Ethernet).

Ad-Hoc mode

An old term used to describe a device-to-device network. (See device-to-device network, peer-to-peer network).

AES

Advanced Encryption Standard. The preferred standard for the encryption of commercial and government data using a symmetric block data encryption technique. It is used in the

implementation of WPA2. (See 802.11i, WPA2).

AP

Access point. A device that connects wireless devices to another network, that being a wireless LAN, Internet Modem or others.

Applet

A small application or utility program, usually written In the Java programming language that is designed to do a very specific and limited task. Applets are most commonly used in hand-held mobile devices.

Application software

A computer program that is designed to do a general operational task such as word processing or payroll. Internet browsers and graphic design programs are also considered applications. Application software runs on top of the operating system.

Association

Describes the establishment and maintenance of the wireless link between devices. (If security is enabled, the devices cannot do anything but exchange security credentials with this link). (See authentication).

Authentication

The process that occurs after association to verify the identity of the wireless device or end user and allow access to the network. (See association, 802.1X, WPA, WPA2).

Backbone

The central part of a large network that links two or more sub-networks. The backbone is the primary data transmission path on large networks such as those of enterprises and service providers. A backbone can be wireless or wired.

Bandwidth

The maximum transmission capacity of a communications channel at any point in time. Bandwidth, usually measured in bits per second (bps), determines the speed at which information can be sent across a network. If you compare the communications channel to a pipe, bandwidth represents the pipe width and determines how much data can flow through the pipe at any one time. The greater the bandwidth, the faster data can flow.

Bluetooth wireless technology

A technology designed for short-range, wireless communications among computing devices and mobile products, including PCs and laptop computers, personal digital assistants, printers, and mobile phones. Designed as a cable-replacement, Bluetooth enables short-range transmission of voice and data in the 2.4 GHz frequency spectrum within a range of about 30 feet. (See WPAN).

Bps

Bits per second. A measure of data transmission speed across a network or communications channel; bps is the number of bits that can be sent or received per second. It measures the speed at which data is communicated and should not be—but often is—confused with bytes per second (Bps, in this reference the B is capitalized while in bps lower case is used). While "bits" is a measure of transmission speed, "bytes" is a measure of storage capacity. (See bandwidth, Mbps).

Bridge

A wireless device that connects multiple networks together. (See router).

Broadband

A comparatively fast Internet connection possessing sufficient bandwidth to accommodate multiple voice, data and video channels simultaneously. Cable, DSL and satellite are all considered to be broadband channels; they provide much greater speed than dial-up Internet access over telephone wires. (See cable modem, DSL).

Broadband modem

A device that connects a local computer or network to a high-speed Internet service, such as DSL or Cable Internet. (See cable modem, DSL).

BSSID

Basic Service Set Identifier. A unique address that identifies the access point/router that creates the wireless network. (See SSID).

Bus adapter

A special adapter card that installs in a PC's PCI or ISA slot and enables the use of PC Card radios in desktop computers. Some companies offer one-piece PCI or ISA Card radios that install directly into an open PC or ISA slot.

Cable modem

A device used with broadband Internet service provided by a traditional cable TV service. Cable modems convert analog data from the cable TV system into a digital format that can be used by a computer. (See broadband modem).

Channel

One portion of the available radio spectrum that all devices on a wireless network use to communicate. Changing the channel on the access point/router can help reduce interference.

Client

Any computer connected to a network that requests files and services (files, print capability) from the server or other devices on the network. The term also refers to end users. (See AP).

Client devices

Wi-Fi client devices include PC Cards that slide into laptop computers, mini-PCI modules embedded in laptop computers and mobile computing devices, as well as USB radios and PCI/ISA bus Wi-Fi radios. Client devices usually communicate with hub devices like access points and gateways. (See AP, client).

Collision avoidance

A means of proactively detecting whether a node on an Ethernet network can transmit a signal without risk that it will collide with other traffic on the network. (See CSMA/CA, CSMA/CD).

Crossover cable

A twisted-pair cable used to network two computers without use of a hub. Instead of traveling in direct parallel paths between plugs, the signals "crossover," reversing the sending and receiving wire pairs on each end. Crossover cables may be required to connect a cable or DSL modem to a wireless router or access point.

CSMA/CA

Carrier Sense Multiple Access/Collision Avoidance. The principal media access control strategy used in 802.11 networks to avoid data collisions. It is a “listen before talk” method of minimizing collisions. The network node checks to see if the transmission channel is clear before a data packet is sent. (See collision avoidance, CSMA/CD).

CSMA/CD

Customer Sense Multiple Access/Collision Detection. The principal media access control

strategy used to manage traffic and reduce noise on wired Ethernet networks. It allows a network device to transmit data after detecting a channel is available. If two devices transmit data simultaneously, the sending device detects the collision of data packets and retransmits after a random time delay. (See collision avoidance, CSMA/CA).

DC power module

Modules that convert Alternate Current (AC) power to Direct Current (DC) for the operation of electronic and computer equipment. Depending on the manufacturer and product, these modules can range from typical "wall wart" transformers that plug into a wall socket to larger, enterprise-level Power Over Ethernet systems that inject DC power into the Ethernet cables to provide power to the access points.

Device-to-device network

Two or more devices that connect using wireless network devices without the use of a centralized wireless access point. Also known as a peer-to-peer network. (See ad hoc mode, Peer-to-peer network).

DHCP

Dynamic Host Configuration Protocol. A protocol for dynamically assigning IP addresses from a pre-defined list to nodes on a network. When they log on, network nodes automatically receive an IP address from a pool of addresses served by a DHCP. The DHCP server provides (or leases) an IP address (to a client for a specific period of time. The client will automatically request a renewal of the lease when the lease is about to run out. If a lease renewal is not requested and it expires, the address is returned to the pool of available IP addresses. Using DHCP to manage IP addresses simplifies client configuration and efficiently utilizes IP addresses. (See IP address).

Dial-up

A connection to a remote network, or the Internet, using a standard modem and telephone connection, or Plain Old Telephone Service (POTS). (See POTS).

Diversity antenna

An antenna system that uses multiple antennas to reduce interference and maximize reception and transmission quality.

DNS

Domain Name Service. An Internet service that translates alphanumeric domain names to assigned IP addresses and vice versa. The term is typically used to describe the server which makes the translation. Every website has its own specific IP address on the Internet. DNS typically refers to a database of Internet names and addresses which

translates the alpha-numeric names to the official Internet Protocol numbers and vice versa. For instance, a DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. (See IP, IP address).

DSL

Digital Subscriber Line. A dedicated digital circuit between a residence or business and a telephone company's central office. It allows high-speed data, voice and video transmissions over existing twisted-pair copper Plain Old Telephone Service (POTS) telephone wires. (See broadband, POTS).

Dual-band

A device that is capable of operating in two frequencies. On a wireless network, dual-band devices are capable of operating in both the 2.4 GHz (802.11b/g) and 5 GHz (802.11a) bands. In cellular phone technology, dual-band devices typically operate in both the GSM900 and GSM1800 frequencies, allowing a greater number of roaming options. (See Tri-mode).

EAP

Extensible Authentication Protocol. A protocol that provides an authentication framework for both wireless and wired Ethernet enterprise networks. It is typically used with a RADIUS server to authenticate users on large networks. EAP protocol types are used in the 802.1X-based authentication in WPA-Enterprise and WPA2-Enterprise. (See 802.1X, EAP, LEAP, RADIUS, TLS, WPA-Enterprise, WPA2-Enterprise).

Encryption

A mechanism for providing data confidentiality. (See 802.11i, RC4, TKIP, WEP, WPA, WPA2).

Enterprise

Any large corporation, business or organization. The enterprise market can incorporate office buildings, manufacturing plants, warehouses and research and development facilities, as well as large colleges and universities.

ESSID

Extended Service Set Identifier. A name used to identify a wireless network. (See SSID, network name).

Ethernet

The most popular international standard technology for wired Local Area Networks (LANs). It provides from 10 Mbps transmission speeds on basic 10BastT Ethernet networks to 100 Mbps transmission speeds on Fast Ethernet networks, 1000 Mbps on Gigabit Ethernet, and 10,000 Mbps on 10 Gigabit Ethernet. (See 802.3)

FIPS 140-2

The Federal Information Processing Standard that defines the requirements of security technologies used in the handling and processing of information within government agencies. (See 802.11i, AES, WPA2).

Firewall

A system of software and/or hardware that resides between two networks to prevent access by unauthorized users. The most common use of a firewall is to provide security between a local network and the Internet. Firewalls can make a network appear invisible to the Internet and can block unauthorized and unwanted users from accessing files and systems on the network. Hardware and software firewalls monitor and control the flow of data in and out of computers in both wired and wireless enterprise, business and home networks. They can be set to intercept, analyze and stop a wide range of Internet intruders and hackers. (See Intrusion detection).

FireWire

A high-speed serial bus system defined by the IEEE 1394 standard for input/output technology that connects multimedia and storage peripherals to a PC. FireWire is similar to USB (Universal Serial Bus) and can provide a bandwidth of about 400 Mbps. FireWire was the original brand name for Apple Computer's implementation of the specification. Today many Windows systems have FireWire capabilities, as well. Other names for products that perform the same function include 1394 (Linux) and iLink (Sony).

Firmware

Software routines that are embedded as read-only memory (ROM) in a computer chip or hardware device to prevent modification of the routines. Unlike random access memory (RAM), read-only memory stays intact in the absence of electrical power. Startup routines and low-level input/output instructions are stored in firmware.

Gateway

In the wireless world, a gateway is an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

GPRS

General Packet Radio Service. A radio technology used in GSM networks that transmits digital data packets, much like Internet protocols do, for both voice and data without the need of a dedicated circuit for always-on access to data. This allows for more efficient communication and faster data rates. (See 3G, GSM).

GPS

Global Positioning System. A system that uses satellites, receivers and software to allow users to determine their precise geographic position. (See War driving).

GSM

Groupe Speciale Mobile, or Global System for Mobile Communications. A 2G digital standard for cellular phone communications adopted by many countries around the world. Its frequency bands range from 900-1800MHz. (See 3G, GPRS).

Hotspot

A location where users can access the Internet using Wi-Fi laptops and other Wi-Fi enabled devices. Access may be provided free or for a fee. Hotspots are often found at coffee shops, hotels, airport lounges, train stations, convention centers, gas stations, truck stops and other public meeting areas. Corporations and campuses often offer it to visitors and guests. Hotspot service is sometimes available aboard planes, trains and boats. (See Wi-Fi ZONE™).

Hub

A multi-port device used to connect client devices to a wired Ethernet network. Hubs can have numerous ports and can transmit data at speeds ranging from 10 to 1000 Mbps per second to all the connected ports. A small wired hub may only connect 4 computers; a large hub can connect 48 or more. (See Router).

HZ

Hertz, not the car rental company. The international unit for measuring frequency equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz; 802.11a devices operate in the 5 GHz band; 802.11b and g devices operate in the 2.4 GHz band.

I/O

Input/Output. The term used to describe any operation that transfers data to or from a computer. (See MIMO).

IEEE

Institute of Electrical and Electronics Engineers. A global technical professional society and standards-setting organization serving the public interest and its members in electrical, electronics, computer, information and other technologies.

IEEE 802.11

The family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 committee which establishes standards for wireless Ethernet networks. 802.11 standards define the over-the-air interface between wireless clients and

a base station, or access point that is physically connected to the wired network. (See 802.11, IEEE).

iLink

Sony Corp's name for the high-speed serial bus system defined by the IEEE 1394 standard for input/output technology that connects multimedia and storage peripherals to a PC. (See FireWire).

Infrastructure mode

An old term used to describe a wireless network consisting of devices connected to a network using a centralized wireless access point. One of two types of wireless network modes; the other is a device-to-device network (also known as peer-to-peer or ad hoc mode). (See ad hoc mode, device-to-device network, peer-to-peer network).

Internet appliance

A computing device used primarily for Internet access. It can be Wi-Fi enabled or connected to a wired network and generally offers customized web browsing, touch-screen navigation, with built-in e-mail services, entertainment and personal information management applications. Applications cannot be installed independently.

Intrusion detection

A security service that monitors and analyzes system events to identify security breaches to the network and provide real-time warnings when an unauthorized intrusion, or break-in, to the network is attempted. (See Rogue, War chalking, War driving).

IP

Internet Protocol. The basic communications protocol of the Internet. (See IP address, TCP/IP).

IP (Internet Protocol) telephony

Technology that supports voice, data and video transmission via IP-based LANs, WANs, and the Internet. This includes VoIP (Voice over IP).

IP address

Internet Protocol address. IP Version 4, the most widely used Internet protocol, provides 32-bit number that identifies the sender or receiver of information sent across the Internet. An IP address has two parts: The identifier of the particular network on the Internet and the identifier of the particular device (which can be a server or a workstation) within that network. The newer IP, Version 6, provides a 128-bit addressing

scheme to support a much greater number of IP addresses. (See DHCP, DNS, IP).

IP telephony

A general term referring to technologies that use IP packet-switched connections to exchange voice, data, video, and other forms of information traditionally carried over public telephone networks. (See IP, VoIP).

IPX-SPX

IPX, short for Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems. Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as SPX and NCP, are used for additional error recovery services. Sequenced Packet Exchange, SPX, a transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications. Whereas the IPX protocol is similar to IP, SPX is similar to TCP. Together, therefore, IPX-SPX provides connection services similar to TCP/IP.

ISA

A type of internal computer bus that allows the addition of card-based components like modems and network adapters. ISA has been replaced by PCI and is not very common anymore.

ISDN

Integrated Digital Services Network—A service offered by most telephone carriers that provides high-speed digital service for voice and data over ordinary telephone lines. ISDN uses standard POTS copper wiring to deliver voice, data or video. (See broadband, POTS).

ISO Network Model

A model developed by the International Standards Organization (ISO) that defines seven levels, or layers, in a network. By standardizing these layers and the interfaces that connect them, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are, beginning at the lowest layer: Physical, Data link, Network, Transport, Session, Presentation, Application. The IEEE 802.11 Standard encompasses the physical layer (PHY) and the lower portion of the data link layer which is often referred to as the Media Access Control (MAC) sub-layer. (See PHY).

ISS

A special software application that allows all PCs on a network access to the Internet simultaneously through a single connection and Internet Service Provider (ISP) account.

LAN

A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN. (See WAN, WLAN, WMAN, WPAN).

LEAP

Lightweight Extensible Authentication Protocol—A proprietary Cisco protocol used for 802.1X authentication on wireless LANs (WLANs). (See 802.1X, EAP).

MAC address

Media Access Control address. A unique hardware number that identifies each device on a network. A device can be a computer, printer, etc. (See IP address).

MAN

Metropolitan Area Network. A data network, typically operated by a municipality or communications carrier that provides high-speed service within a geographical area such as a college campus, town or city. A MAN is larger than a Local Area Network (LAN) but smaller than a Wide Area Network (WAN). (See WiMAX).

Mapping

Assigning a PC to a shared drive or printer port on a network.

Mbps

Megabits per second. A measurement of data speed that is roughly equivalent to a million bits per second. (See bps).

Mesh network

A communications network with least two pathways to each node, forming a net-like organization. When each node is connected to every other node, the network is said to be fully meshed. When only some of the nodes are linked, switching is required to make all the connections and the network is said to be partially meshed, or partially connected.

MIC

Message Integrity Check. A technology that is employed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If it does not match, the data is assumed to have been tampered with and the packet is dropped. (See Packet, TKIP, WPA, WPA2).

MIMO

Multiple-Input-Multiple-Output. An advanced signal processing technology that uses multiple receivers and multiple transmitters in both the client and access point to achieve data throughput speeds of 100Mbps. (See 802.11n).

Mobile professional

Often called "road warrior." Any employee or professional person who travels frequently and requires the ability to regularly access his or her corporate networks, via the Internet, to post and retrieve files and data and to send and receive e-mail from remote locations. (See hotspot, roaming).

NAT

Network Address Translation. A network capability that enables multiple of computers to dynamically share a single incoming IP address from a dial-up, cable or DSL connection. NAT takes a single incoming public IP address and translates it to a new private IP address for each client on the network. (See DHCP, IP address).

Network name

A name used to identify a wireless network. (See ESSID, SSID)

NIC

Network Interface Card. A wireless or wired PC adapter card that allows the client computer to utilize network resources. Most office wired NICs operate at 100 Mbps. Wireless NICs operate at data rates defined by 802.11 standards. (See PC card).

Packet

A unit of information transmitted from one device to another on a network. A packet typically contains a header with addressing information, data, and a checksum to insure data integrity. (See MIC).

Pass phrase

A series of characters used to create a key which is used by Wi-Fi Protected Access (WPA). (See PSK, WPA).

PC Card

A removable, credit-card-sized memory or I/O device that fits into an expansion slot on a notebook computer or a personal digital assistant (PDA). PC Cards are used primarily in notebook computers and PDAs. PC Card peripherals include Wi-Fi network cards, memory cards, modems, wired NICs, and hard drives. (See NIC, PCI).

PCI

Peripheral Component Interconnect. A high-performance I/O (input/output) computer bus that allows expansion slots to be spaced closely for high-speed operation. (See NIC, PC Card).

PCMCIA

Expansion cards now referred to as "PC Cards" were originally called "PCMCIA Cards" because they met the standards created by the Personal Computer Memory Card International Association.

PDA

Personal Digital Assistant. Smaller than laptop computers but with many of the same computing and communication capabilities, PDAs range greatly in size, complexity and functionality. PDAs can provide wireless connectivity via embedded Wi-Fi Card radios, slide-in PC Card radios, or Compact Flash Wi-Fi radios. (See PC Card).

PEAP

PEAP—Protected Extensible Authentication Protocol. A protocol proposed by Microsoft, Cisco and RSA Security for 802.1X authentication on wireless LANs (WLANs). (See EAP, LEAP).

Peer-to-peer network

A wireless or wired computer network that has no server or central hub or router. All the networked PCs are equally able to act as a network server or client, and each client computer can talk to all the other wireless computers without having to go through an access point or hub. However, since there is no central base station to monitor traffic or provide Internet access, the various signals can collide with each other, reducing overall performance. (See Ad hoc mode, Device-to-device network).

PHY

The physical, or lowest, layer of the OSI Network Model. In a wireless network, the PHY defines parameters such as data rates, modulation method, signaling parameters, transmitter/receiver synchronization, etc. Within an actual radio implementation, the

PHY corresponds to the radio front end and baseband signal processing sections. (See ISO Network Model).

Plug-and-play

Features that provide for automatic configuration of add-ons and peripheral devices such as wireless PC Cards, printers, scanners and multimedia devices. (See PC Card).

POTS

Plain Old Telephone Service. The traditional analog telephone service provided by most common carriers. (See broadband, dial-up, DSL, ISDN).

Print server

A network device, often a computer, that connects to at least one printer, allowing it to be shared among computers on a network.

Proxy server

A technique used in larger companies and organizations to improve network operations and security. The proxy server receives requests intended for another server to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.

PSK

A mechanism in Wi-Fi Protected Access (WPA)—Personal that allows the use of manually entered keys or passwords to initiate WPA security. The PSK is entered on the access point or home wireless gateway and each PC that is on the Wi-Fi network. After entering the password, Wi-Fi Protected Access automatically takes over. It keeps out eavesdroppers and other unauthorized users by requiring all devices to have the matching password. The password also initiates the encryption process which, in WPA is Temporal Key Integrity Protocol (TKIP) and in WPA2 is Advanced Encryption Standard (WPA2). (See TKIP, WPA-Personal, WPA2-Personal).

QoS

Quality of Service. Required to support wireless multimedia applications and advanced traffic management. QoS enables Wi-Fi access points to prioritize traffic and optimize the way shared network resources are allocated among different applications. Without QoS, all applications running on different devices have equal opportunity to transmit data frames. That works well for data traffic from applications such as web browsers, file

transfers, or e-mail but it is inadequate for multimedia applications. Voice over Internet Protocol (VoIP), video streaming, and interactive gaming are highly sensitive to latency increases and throughput reductions and require QoS. QoS extensions for 802.11 networks will be addressed in the upcoming IEEE 802.11e standard. (See 802.11e, WMM).

RADIUS

Remote Access Dial-Up User Service. A standard technology used by many major corporations to protect access to wireless networks. RADIUS is a user name and password scheme that enables only approved users to access the network; it does not affect or encrypt data. The first time a user wants access to the network, secure files or net locations, he or she must input his or her name and password and submit it over the network to the RADIUS server. The server then verifies that the individual has an account and, if so, ensures that the person uses the correct password before she or he can get on the network. RADIUS can be set up to provide different access levels or classes of access. For example, one level can provide blanket access to the Internet; another can provide access to the Internet as well as to e-mail communications; yet another account class can provide access to the Net, email and the secure business file server. Like other sophisticated security technologies, RADIUS comes in a variety of types and levels. (See EAP, WPA, WPA2).

Range

The distance covered by a wireless network or radio device. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to a mile.

RC4

An encryption cipher designed RSA Data Security. It allows key lengths up to 1024 bits and is a component in many encryption schemes, including SSL, WEP, and TKIP. (See SSL, WEP, TKIP).

Repeater

A wireless repeater is a device that extends the coverage of an existing access point by relaying its signal. A wireless repeater does not do intelligent routing performed by wireless bridges and routers.

Residential gateway

A wireless device that allows multiple devices accessing a home network, including PCs and peripherals to access the Internet and communicate with one another. (See gateway).

RFID

Radio Frequency Identification. An electronic identification technology that uses radio frequency signals to read identifying data contained in tags on equipment and merchandise. An alternative to bar codes.

RJ-45

Standard connectors used in Ethernet networks. They appear similar to standard RJ-11 telephone connectors. However, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Roaming

The ability to move seamlessly from one area of Wi-Fi or cellular phone coverage to another with no loss in connectivity. Roaming also refers to the ability of road warriors to wirelessly connect to the Internet from different hotspots without confronting the array of schemes used by different providers to authorize use and track billing. Roaming agreements among providers allow mobile professionals to a single authentication and authorization scheme to have all charges resolved to a single bill. (See hotspot, mobile professional).

Rogue

An unauthorized access point installed on a company's WLAN, typically by a user. Rogue access points present security risks. They rarely conform to the organization's security policies and, typically, no security at all is enabled on them. Rogues present open, insecure interfaces to the company's network. (See intrusion detection).

Router

A wireless router is a device that accepts connections from wireless devices to a network and includes a network firewall for security, and provides local network addresses. (See hub).

Satellite broadband

Wireless high-speed Internet service provided by satellites. Some satellite broadband connections are two-way—up and down. Others are one-way, with the satellite providing a high-speed downlink and then using a dial-up telephone connection or other land-based system for the uplink to the Internet. (See broadband, dial-up).

Security supplicant

Client software that coordinates authentication and session key creation.

Server

A computer that provides resources or services to other computers and devices on a network. Types of servers can include print servers, Internet servers, mail servers, and DHCP servers. A server can also be combined with a hub or router. (See DHCP, hub, router).

Site survey

A comprehensive facility study performed by network managers to insure that planned service levels will be met when a new wireless LAN, or additional WLAN segments to an existing network, are deployed. Site surveys are usually performed by a radio frequency engineer and used by systems integrators to identify the optimum placements of access points to insure that planned levels of service are met. Site surveys are sometimes conducted following the deployment to insure that the WLAN is achieving the necessary level of coverage. Site surveys can also be used to detect rogue access points. (See intrusion detection, rogue).

Sniffer

A software program that monitors network traffic. Sniffers can capture data being transmitted on a network and are sometimes used illegitimately to hack a network.

SOHO

The term describes an office or business with ten or fewer computers and/or employees.

SSID

A unique 32-character network name, or identifier, that differentiates one wireless LAN from another. All access points and clients attempting to connect to a specific WLAN must use the same SSID. The SSID can be any alphanumeric entry up to a maximum of 32 characters. (See ESSID, network name).

SSL

SSL—Secured Sockets Layer. A protocol used to secure Internet communications. SSL is commonly used to encrypt transactions on online retail and banking. SSL encrypts the exchange of information between a user's browser and Web server so only the intended parties can read it. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session. (See RC4).

Subnetwork, or subnet

An IP address range that is part of a larger address range. Subnets are used to subdivide a network address of a larger network into smaller networks. Subnets connect to other networks through a router. Each individual wireless LAN will typically use the same subnet for all of its clients. (See IP address, router).

Switch

A type of hub that controls device usage to prevent data collisions and insures optimal network performance. A switch acts as a network traffic cop: Rather than transmitting all the packets it receives to all ports, as a hub does, a switch transmits packets to only the receiving port. (See hub).

TCP

Transmission Control Protocol. The Transport level protocol used with the Internet Protocol (IP) to route data across the Internet. (See IP, TCP/IP).

TCP/IP

The underlying technology of Internet communications. While IP handles the actual delivery of data, TCP tracks the data packets to efficiently route a message through the Internet. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup (See DHCP) or permanently assigned as a static address. All TCP/IP messages contain the address of the destination network, as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide. For example, when a user downloads a web page, TCP divides the page file on the web server into packets, numbers the packets, and forwards them individually to the user's IP address. The packets may be routed along different paths before reaching the user's address. At the destination, TCP reassembles the individual packets, waiting until they have all arrived to present them as a single file. (See IP, IP address, packet, TCP).

Throughput

Usually measured in bps, Kbps, Mbps or Gbps, throughput is the amount of data that can be sent from one location to another in a specific amount of time. (See bps, Mbps).

TKIP

Temporal Key Integrity Protocol. The wireless security encryption mechanism in Wi-Fi Protected Access. TKIP uses a key hierarchy and key management methodology that removes the predictability that intruders relied upon to exploit the WEP key. It increases the size of the key from 40 to 128 bits and replaces WEP's single static key with keys that are dynamically generated and distributed by an authentication server, providing some 500 trillion possible keys that can be used on a given data packet. It also includes a Message Integrity Check (MIC), designed to prevent an attacker from capturing data packets, altering them and resending them. By greatly expanding the size of keys, the number of keys in use, and by creating an integrity checking mechanism, TKIP magnifies the complexity and difficulty involved in decoding data on a Wi-Fi network. TKIP greatly increases the strength and complexity of wireless encryption, making it far more difficult—if not impossible—for a would-be intruder to break into a Wi-Fi network. (See

AES, WPA, WPA2).

TLS

Transport Layer Security. A newer version of the SSL protocol. It supports more cryptographic algorithms than SSL. TLS is designed to authenticate and encrypt data communications, preventing eavesdropping, message forgery and interference. (See EAP, SSL).

Tri-mode

In the Wi-Fi context, tri-mode refers to devices which are 802.11b, a, and g-compatible. In the mobile context, tri-mode describes a cellular phone that is capable of using analog, digital and GSM frequencies. (See dual band).

USB

A high-speed bidirectional serial connection between a PC used to transfer data between the computer and peripherals such as digital cameras and memory cards. The USB 2.0 specification, announced in 2000, provides a data rate of up to 480 Mbps, 40 times faster than the original specification which provided only 12 Mbps.

UWB

Ultra Wideband. A relatively new term that is used to describe a technology known since the early 1960s as "carrier-free", "baseband" or "impulse". UWB transmits and receives extremely short bursts of radio signals, typically a few trillionths of a second to a few billionths of a second (nanoseconds) in duration. These bursts produce waveforms that are extremely broadband.

Voice over Wi-Fi

VoIP services delivered over wireless networks. Sometimes referred to as wireless voice over IP. (See IP telephony, VoIP).

VoIP

Voice over Internet Protocol. A technology for transmitting ordinary telephone calls over the Internet using packet-based networks instead of standard public switched telephone networks or Plain Old Telephone Service (POTS). (See IP telephony, Voice over Wi-Fi).

VPN

Virtual Private Network. A network layer encryption scheme that allows remote clients to securely connect to their corporate networks using the Internet. Most major corporations today use VPN to protect their remote-access workers and their connections. It works by

creating a secure virtual "tunnel" from the end-user's computer through the end-user's access point or gateway, through the Internet, all the way to the corporation's servers and systems. It also works for wireless networks and can effectively protect transmissions from Wi-Fi equipped computers to corporate servers and systems.

WAN

Wide Area Network (WLAN). A data communications network that spans large local, regional, national or international areas and is usually provided by a public carrier (such as a telephone company or service provider).The term is used to distinguish between phone-based data networks and Wi-Fi networks. Phone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks. (See LAN, WMAN, WPAN).

WAP

Wireless Applications Protocol. A protocol designed to deliver applications to mobile devices, including cell phones, pagers, two-way radios, smartphones and communicators.

War chalking

The practice of indicating the presence of both secured and unsecured wireless networks by using chalk to mark nearby buildings or sidewalks.

War driving

The practice of driving around with a GPS, laptop equipped with WNIC and an antenna (usually built into the WNIC) to document the location of secured and unsecured WLANs. The locations of the WLANs derived from the GPS readings, and their corresponding SSIDs, are published in databases that live on the Internet. War driving derives its name from the movie, War Games, in which hackers gained access to traditional networks by randomly dialing telephone numbers until a modem answered. (See GPS).

WEP

The original security standard used in wireless networks to encrypt the wireless network traffic. (See WPA).

Wi-Fi CERTIFIED™

The certification standard designating IEEE 802.11-based wireless local area network (WLAN) products that have passed interoperability testing requirements developed and governed by the Wi-Fi Alliance. (See Wi-Fi Interoperability Certificate).

Wi-Fi Interoperability Certificate

A statement that a product has passed interoperability testing and will work with other Wi-Fi CERTIFIED products. (See Wi-Fi CERTIFIED).

Wi-Fi ZONE™

A certification program of the Wi-Fi Alliance that allows users to easily identify public hotspot locations that have Wi-Fi connectivity available. The program allows customers from anywhere in the world to look for a single Wi-Fi ZONE brand. The Wi-Fi ZONE logo assures users that they will be able to get a fast, reliable Internet connection in a coffee shop, hotel, airport, convention center or other public venue. (See hotspot).

Wi-Fi®

Short for wireless fidelity. A term developed by the Wi-Fi Alliance to describe wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. (See Wi-Fi CERTIFIED™).

WiMAX

Worldwide Interoperability for Microwave Access. Refers to the 802.16 standard being developed by the IEEE to provide a wireless coverage of up to 31 miles. It operates in the 2 to 11 GHz bands and enables connectivity without a direct line-of-sight to a base station although line-of-site is probably required to achieve connectivity at the distance of 31 miles.. It provides shared data rates up to 70 Mbps, which, according to WiMAX proponents, is enough bandwidth to simultaneously support more than 60 businesses and hundreds of homes. (See WMAN).

Wireless network

Devices connected to a network using a centralized wireless access point. (See WLAN).

WLAN

Wireless Local Area Network. A type of local-area network in which data is sent and received via high-frequency radio waves rather than cables or wires. (See LAN, wireless network).

WMAN

Wireless Metropolitan Area Network—A wireless data network that is comparable to a cell phone network in that users throughout a metropolitan area can freely access the Internet. WiMAX technology provides the basis of WMAN networks. (See WiMAX).

WMM™

Wi-Fi Multimedia. A group of features for wireless networks that improve the user experience for audio, video and voice applications. WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority. (See 802.11e, QoS).

WPA-Enterprise

Wi-Fi Protected Access–Enterprise. A wireless security method that provides strong data protection for multiple users and large managed networks. It uses the 802.1X authentication framework with TKIP encryption and prevents unauthorized network access by verifying network users through an authentication server. (See 802.1X, TKIP, WPA).

WPA-Personal

Wi-Fi Protected Access–Personal. A wireless security method that provides strong data protection and prevents unauthorized network access for small networks. It uses TKIP encryption and protects against unauthorized network access through the use of a pre-shared key (PSK). (See WPA, PSK).

WPA™

Wi-Fi Protected Access. An improved security standard for wireless networks that provides strong data protection and network access control. WPA was developed by the Wi-Fi Alliance and addresses all known WEP vulnerabilities. It provides strong data protection by using encryption, as well as strong access controls and 802.1X-based user authentication which was largely missing in WEP. WPA is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, dual-band and tri-mode. WPA can be enabled in two versions, WPA-Personal and WPA-Enterprise. WPA-Personal protects against unauthorized network access by utilizing a set-up pass phrase, or pre-shared key. WPA-Enterprise verifies network users through an authentication server. In either mode, WPA utilizes 128-bit encryption keys and dynamic session keys to ensure the wireless network's privacy and security. (See PSK, WEP, WPA2).

WPA2-Enterprise

Wi-Fi Protected Access 2 – Enterprise. The follow on wireless security method to WPA that provides stronger data protection for multiple users and large managed networks. It prevents unauthorized network access by verifying network users through an

authentication server. (See WPA2).

WPA2-Personal

Wi-Fi Protected Access 2 – Personal. The follow on wireless security method to WPA that provides stronger data protection and prevents unauthorized network access for small networks. (See WPA2, PSK).

WPA2™

Wi-Fi Protected Access 2. The follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the ratified IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1X-based authentication. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA. Like WPA, WPA2 uses the 802.1X/EAP framework as part of the infrastructure that ensures centralized mutual authentication and dynamic key management and offers a pre-shared key for use in home and small office environments. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, multi-band and multi-mode. (See WPA2-Enterprise, WPA2-Personal).

WPAN

Wireless Personal Area Network. A network that wirelessly connects personal devices centered within a radius of about 30 feet such as an individual's workspace or room environment in a home. WPAN technologies include Bluetooth and others defined by the IEEE 802.15 standard. Devices specifications include low data rates (250 kbps, 40 kbps, and 20 kbps), and multi-month to multi-year battery life and include such things as joy sticks and interactive toys. WPAN devices operate in unlicensed international frequency bands and can communicate directly with one another, a concept called "plugging in". (See Bluetooth wireless technology).

References

1 J. Walker, Unsafe at Any Key Size: An Analysis of the WEP Encapsulation, IEEE Submission. (October, 2000)

2 William Stallings, Wireless Communications and Networks, 1st edition (August 6, 2001), Prentice Hall; ISBN: 0201634422

3 IEEE Network (technical journal)

4 Bluesocket Whitepaper, Welcome to the Fourth Generation of Wireless LANs Network World Electronic Newsletter, (February 9, 2005)

5 William Stallings, Local and Metropolitan Networks, 6th edition (August 6, 2001), Prentice Hall; ISBN: 0-13-012939-0

6 Frank Hanzlik, Wi-Fi Alliance Introduces Next Generation of Wi-Fi® Security, Wi-Fi Alliance Press Release (September 1, 2004)

7 Andy Dornan, Emerging Technology: Wireless Security – Is Protected Access Enough? Network Magazine, (October 6, 2003)

8 Belgacom Whitepaper, Security for Enterprises in the 21st Century, Network World Electronic Newsletter, (February 9, 2005)

9 John Edney and William A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison Wesley, (2003)

10 Andy Dornan, The Essential Guide to Wireless Communications Applications, 2004, Prentice Hall, ISBN 013-0097-187

11 Network Defense, Network Magazine, (September 2003)

12 Roadblocks for War Drivers: Stop Wi-Fi from Making Private Networks Public, Network Magazine, (December 2002)

13 William Stallings, Data and Computer Communications, 7th edition, Pearson Education, Upper Saddle River, NJ, 2004.

14 Wi-Fi Alliance. Available online: http://www.wi-fi.org/.

15 Glenn Fleishman, What is Wi-Fi? August 1, 2003. Available online: http://wifinetnews.com/archives/000977.html#nancy.

16 Behrouz A. Forouzan, Data Communications and Networking, 3rd edition, McGraw-Hill, New York, NY, 2004.

17 Enterprise Solutions for Wireless LAN Security, Wi-Fi Alliance, February 6, 2003. Available online: http://www.wi-fi.org/opensection/pdf/whitepaper_wi-fi_enterprise2-6-03.pdf

18 Seth Fogie, Cracking Wi-Fi Protected Access (WPA), Part 2 , March 11, 2005, Available online: http://www.informit.com/articles/article.asp?p=370636)