Wi-Fi Protected Access:
Strong, standards-based, interoperable security for today's Wi-Fi networks

Wi-Fi Alliance
April 29, 2003

Executive Summary

The Wi-Fi Alliance, working in conjunction with the Institute of Electrical and Electronics Engineers (IEEE), has brought a strong interoperable Wi-Fi security specification to market in the form of Wi-Fi Protected Access (WPA).

WPA greatly increases the level of over-the-air data protection and access control on existing and future Wi-Fi networks. It addresses all known weaknesses of Wired Equivalent Privacy (WEP), the original native security mechanism in the 802.11 standard.

Although no security solution can claim to be "bullet-proof," WPA represents a quantum leap forward in Wi-Fi security. WPA is built on standards-based interoperable security enhancements. It brings forward features of the forthcoming IEEE 802.11i standard that can be implemented immediately. WPA not only provides strong data encryption to correct WEP's weaknesses, it adds 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, multi-band and multi-mode. As a subset of 802.11i (also known as WPA2), WPA is both forward and backward-compatible and is designed to run on existing Wi-Fi devices as a software download. .As such, WPA devices should work well with the WPA2 devices expected to appear in the market in 2004.

The Wi-Fi Alliance, which conducts interoperability tests on Wi-Fi devices, is now testing devices for WPA interoperability. These will appear in the market in the second quarter of 2003.

WPA is designed to provide best-in-class enterprise security. At the same time, it offers a mode for small office and home-based networks. It will fully replace WEP as the Wi-Fi security solution.

WPA, when properly installed, provides users of wireless local area networks (WLANs) with a high level of assurance that their data will remain protected and that only authorized users can access their networks.

With WPA, companies that have been using add-on security mechanisms, such as virtual private networks (VPNs) and other proprietary technologies to bolster security on their Wi-Fi networks will find that these are no longer needed—at least not to secure the wireless segments of the network.

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless local area network products based on IEEE 802.11 specifications. Wi-Fi product certification began in March of 2000. One of the goals of the Wi-Fi Alliance is to ensure that consumers realize maximum benefit from their Wi-Fi products in a secure and productive environment.

Table of Contents

I. OVERVIEW

Over the past year, the Wi-Fi Alliance has spearheaded an effort to bring to market a standards-based interoperable security specification that would greatly increase the level of data protection and access control for Wi-Fi wireless local area networks. That specification is Wi-Fi Protected Access (WPA).

WPA addresses the flaws in Wired Equivalent Privacy (WEP), the original native security mechanism for WLANs that has been in place since the adoption of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard in 1997. By 2001, WEP's cryptographic weaknesses had become well-known. A series of independent studies from various academic and commercial institutions had shown that an intruder equipped with the proper tools and a moderate amount of technical knowledge could gain unauthorized access to a WLAN even with WEP enabled.

In spite of its flaws, WEP did provide a margin of security compared to no security at all. It remained useful for deflecting eavesdroppers in home and small office/home office (SOHO) environments where network traffic is light. However, it was not sufficient for enterprise use. Many large companies strengthened WEP by deploying it with other third-party security solutions, including virtual private networks (VPNs), 802.1X authentication servers, and other proprietary technologies.

Concerned that the lack of strong native wireless security would hinder the adoption of Wi-Fi devices into the market, the Wi-Fi Alliance, in conjunction with the IEEE, initiated an effort to bring a strongly improved, standards-based, interoperable Wi-Fi security solution to market.

WPA is that solution. WPA is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, multi-band and multi-mode.

WPA is a subset of the IEEE's forthcoming 802.11i standard (also known as WPA2) that is expected to be ratified in the first quarter of 2004. As such, it is forward-and backward-compatible with WPA2. WPA will be viable in the market for many years to come and should work comfortably with WPA2 devices as they become available.

WPA addresses Wi-Fi security with a strong new encryption algorithm as well as user authentication, a feature that was largely missing in WEP. When properly installed, it provides a high level of assurance that user data will remain protected and that only authorized users may access the network. With WPA enabled, enterprises can offer employees the ease and flexibility of working wirelessly and securely without deploying add-on security solutions, such as VPNs.

Enterprise users as well as those at home and in SOHO environments, have a strong security for their network. Wireless Internet service providers (WISPs) may also find that WPA's enhanced encryption and authentication schemes are attractive in public "hot spots" as they provide a high level of security for service providers and mobile users who are not utilizing VPN connections.

II. WPA AT A GLANCE

WPA addresses all known vulnerabilities in WEP to ensure data authenticity on wireless LANs and protect against even the most targeted hacker attacks. It is designed to

minimize impact on network performance and to run as a software upgrade on the more than 650 Wi-Fi CERTIFIED products in today's market.

Cryptographers have reviewed Wi-Fi Protected Access and have verified that it meets its claims to close all known WEP vulnerabilities and provides an effective deterrent against known attacks.

WPA uses the Temporal Key Integrity Protocol (TKIP) for encryption and employs 802.1X authentication with one of the standard Extensible Authentication Protocol (EAP) types available today.

The Wi-Fi CERTIFIED logo with a checked box next to Wi-Fi Protected Access means that the Wi-Fi Alliance has tested and certified WPA interoperability in the product.

WPA can be installed as a software upgrade on most current Wi-Fi devices. Access points (APs) require a software upgrade. Client workstations require a software upgrade to the network interface card (NIC) and a possible software upgrade to the operating system. Enterprises will require an authentication server (typically a Remote Authentication Dial-In User Service, or RADIUS server). WPA accommodates home and SOHO users who do not have such servers available with a special mode that uses a shared password to activate WPA protection.

The Wi-Fi Alliance has begun certifying WPA products. Initial shipments are expected to begin mid-year with many other products to follow. WPA will be optional in Wi-Fi CERTIFIED products during an initial phase-in period. WPA security will be indicated in the Wi-Fi certification logo on products that possess it.

WPA will fully replace WEP as the security solution in new Wi-Fi devices. It will become mandatory for selected PC products to earn Wi-Fi certification by the end of 2003.

III. TRANSITIONING TO WPA IN THE ENTERPRISE

WPA presents a natural migration path for currently installed devices. Enterprises that are presently using 802.1X/EAP authentication can upgrade to WPA without forfeiting their investment. IT managers are advised to ensure that WPA is present in new Wi-Fi devices that are purchased and to update WEP-based installations at both AP and client workstations to WPA. For enterprise networks, implementing Wi-Fi Protected Access will involve deploying an 802.1X infrastructure. This implies:

- Selection of EAP types that will be supported on client NICs and authentication servers.
- Selection and deployment of an authentication server, typically a Remote Authentication Dial-In User Service (RADIUS) server.
- Upgrade of APs with Wi-Fi Protected Access or purchase new APs with WPA installed.

- Upgrade of WLAN-client NICs with Wi-Fi Protected Access or purchase new wireless NICs with WPA installed.

In large enterprise settings, it is likely that access points will be upgraded before all the upgrades at client workstations can be completed. For this reason, some vendors plan to offer a "mixed mode" on access points to support WPA, as well as clients running original WEP security. While this mixed mode may be useful during a transition, it is fundamentally insecure. WEP clients will continue to present open portholes through which intruders can access the wireless network. The net effect of mixed mode operation is that a WPA network will be no more secure than if it were running WEP security alone.

Mixed mode is not a feature of WPA. The Wi-Fi Alliance does not test it for interoperability and does not recommend its use. Large organizations that use it should accelerate the transition to WPA, using mixed mode for the shortest possible period of time. Enterprises that are currently using VPN or other vendor-specific 802.1X/EAP solutions should continue their use through the upgrade period. After transitioning to Wi-Fi Protected Access, most enterprises will not find a need for these additional technologies, at least not for the specific purpose of securing the Wi-Fi network.

VPN remains a complimentary technology that will co-exist well with WPA to secure remote connections, such as those of users who access a corporate network through a public wireless Internet access services.

IV. SECURITY MECHANISMS IN WPA

One of WEP's chief weaknesses was that it used a small static key to initiate encryption. This 40-bit key is entered manually on the AP and on all clients that communicate with the AP. It does not change unless it is manually re-entered on all devices, a daunting labor-intensive task in a large organization.

Cryptographic studies have demonstrated that an intruder who collects enough data can threaten a WEP network in three ways: by intercepting and decrypting the data that is being transmitted over the air, by altering the data that is communicated, and by deducing and forging the WEP key to gain unauthorized access to network and Internet services. This could be accomplished in a matter of hours on a busy, corporate WLAN. Also, WEP lacks a means of authentication, validating user credentials to ensure that only those who should be on the network are allowed to access it. WPA addresses these flaws and brings additional safeguards to Wi-Fi security.

WPA uses a greatly enhanced encryption scheme, Temporal Key Integrity Protocol (TKIP). Together with 802.1X/EAP authentication, TKIP employs a key hierarchy that greatly enhances protection. It also adds a Message Integrity Check (MIC, sometimes called "Michael") to protect against packet forgeries.

WEP v. WPA

	WEP	WPA
Encryption	Flawed, cracked by scientists and hackers	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static – same key used by everyone on the network	Dynamic session keys. Per user, per session, per packet keys
	Manual distribution of keys – hand typed into each device	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1X and EAP

Encryption

TKIP 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 the authentication server. TKIP uses a key hierarchy and key management methodology that removes the predictability which intruders relied upon to exploit the WEP key.

To do this, TKIP leverages the 802.1X/EAP framework. The authentication server, after accepting a user's credentials, uses 802.1X to produce a unique master, or "pair-wise" key for that computing session. TKIP distributes this key to the client and the AP and sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated during that user's session. TKIP's key hierarchy exchanges WEP's single static key for some 500 trillion possible keys that can be used on a given data packet.

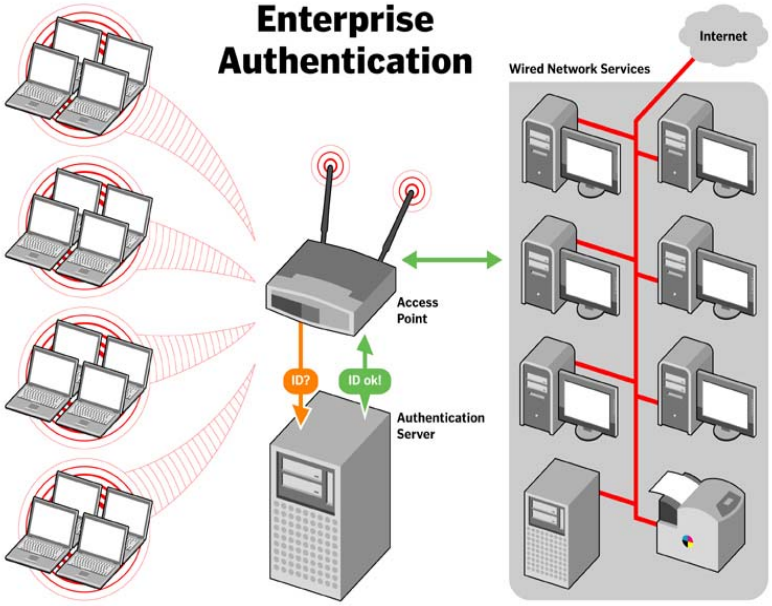
The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, the data is assumed to have been tampered with and the packet is dropped.

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.

Designed to be deployed with existing Wi-Fi CERTIFIED devices, TKIP is also included in the proposed WPA2 standard.

Authentication

WPA uses 802.1X authentication with one of the Extensible Authentication Protocol (EAP) types available today. 802.1X is a port-based network access control method for wired, as well as wireless, networks. It was adopted as a standard by the IEEE in August of 2001.

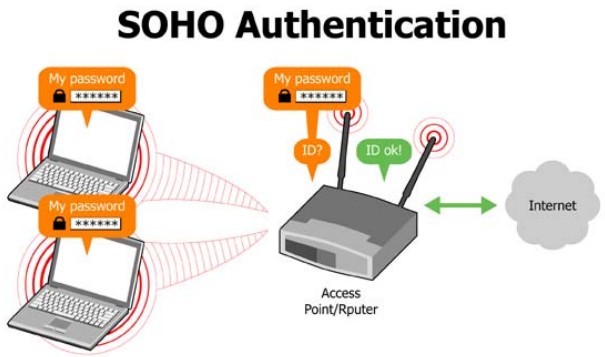


EAP handles the presentation of users' credentials, in the form of digital certificates (already widely used in Internet security), unique usernames and passwords, smart cards, secure IDs, or any other identity credential that the IT administrator is comfortable deploying. WPA allows flexibility in both the type of credentials that are used and in the selection of an EAP type. A wide number of standards-based EAP implementations are available for use, including EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), and Protected Extensible Authentication Protocol (PEAP).

With EAP, 802.1X creates a framework in which client workstations mutually authenticate with the authentication server. This mutual authentication prevents users from accidentally connecting to "rogue" or unauthorized APs on the Wi-Fi network and also ensures that users who access the network are the ones who are supposed to be there. When a user requests access to the network, the client sends the user's credentials to the authentication server via the AP. If the server accepts the user's credentials, the master TKIP key is sent to both the client and to the AP. A four-way handshake, a process in which the client and AP acknowledge one another and install the keys, completes the process

Security for homes and small offices

Users in small office and home office (SOHO) environments lack the budget and IT staff to install and maintain RADIUS authentication servers. WPA recognizes this by offering these users the benefits of WPA security through the use of a "pre-shared key" (PSK) or password.



The PSK provides home and SOHO users with the same strong TKIP encryption, per-packet key construction, and key management that WPA provides in the enterprise.

The difference is that here, a password is manually entered on client devices and on the AP or wireless gateway and used for authentication. While not as robust as a full-blown RADIUS, EAP and 802.1X authentication approach, the PSK provides a useful alternative for smaller networks.

Upgrading to Wi-Fi Protected Access in home and small office environments is simple. Users can purchase new WPA-enabled equipment or update installed equipment. For most users, the update is as easy as installing a new hardware driver.

The steps are:

- Upgrade the APs with WPA software.
- Upgrade the WLAN network interface cards with Wi-Fi Protected Access software.
- Configure the PSK, or master password, on the AP.
- Configure the PSK on client workstations.

V. THE FUTURE: WPA2

TKIP encryption, 802.1X/EAP authentication and PSK technology in WPA are features that have been brought forward from WPA2. Additionally, WPA2 will provide a new, encryption scheme, the Advanced Encryption Standard (AES).

AES has already been adopted as an official government standard by the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST). AES will be defined in counter cipher-block chaining mode (CCM) and will support the Independent Basic Service Set (IBSS) to enable security between client workstations operating in ad hoc mode. AES uses a mathematical ciphering algorithm that employs variable key sizes of 128-, 192- or 256-bits.

Like WPA, WPA2 will use the 802.1X/EAP framework as part of the infrastructure that ensures centralized mutual authentication and dynamic key management. It, too, 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.

Enterprises building new WLANs will find AES attractive. However, in many cases it will require new investments in hardware. Thus, the business must weigh the benefits of the enhanced security that WPA2 offers against the cost of new equipment.

There is no reason not to upgrade now to WPA. While a hardware upgrade may be needed to deploy the AES portion of WPA2 on WPA-enabled devices, the 802.1X authentication, TKIP encryption, and PSK components of Wi-Fi Protected Access make the two specifications quite compatible.

WPA2 offers a graceful transition path from WPA that presents a compelling case for upgrading to WPA now. WPA2 will offer a highly secure “mixed mode” that supports both WPA and WPA2 client workstations. This will allow for an orderly transition in large enterprises that cannot readily upgrade in a short period of time.

Unlike the WEP/WPA mixed mode in WPA devices, WPA2’s mixed mode will support both WPA and WPA2. It delivers a high level of security to enterprises as they make the move to the even higher level of security offered in WPA2. Since Wi-Fi Protected Access already provides strong encryption, the transition to WPA2 clients and APs can be done gradually, seamlessly, and with a high level of confidence that security will not be compromised.

VI. SUMMARY AND CONCLUSIONS

Wi-Fi Protected Access fixes all known vulnerabilities in Wi-Fi network security and greatly enhances data protection and access control on existing and future Wi-Fi wireless LANs. It provides an immediate, strong, standards-based, interoperable security solution that addresses all known flaws in the original WEP-based security. IT enterprises, small offices and users at home can purchase new or upgrade existing, Wi-Fi CERTIFIED devices with the WPA CERTIFIED mark, secure in the knowledge that their networks will be protected.

As a subset of WPA2, WPA presents users with a solution that is both forward- and backward-compatible with present and future wireless standards. It offers enterprise-grade protection and, most importantly, it is available today.

WPA allows users, whether they are at home or at work, to enjoy all the mobility and flexibility that Wi-Fi wireless computing has to offer, knowing that their data is safely protected beyond the reach of intruders.