Meetinghouse
DATA COMMUNICATIONS

White Paper

A Meetinghouse Whitepaper

WPA: A Key Step Forward in Enterpriser-class Wireless LAN (WLAN) Security

By **Jon A. LaRosa, VP, Engineering**

Table of Contents

Executive Summary

Wireless LAN (WLAN) technology is desirable to the enterprise because of the mobility it can provide to end users. However, enterprise-class security for these systems has been elusive. To address the enterprise security problem IEEE introduced the Wired Equivalent Privacy (WEP). This optional security measure was meant to secure 802.11b (Wi-Fi) WLANs, but inherent weaknesses in the standard soon became obvious.

In response to this situation, the Wi-Fi Alliance announced a new security architecture in October 2002 that remedies the short comings of WEP. This standard, formerly known 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 being defined in the 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 as enterprise-class security is realized.

WPA works with existing 802.11-based hardware (although firmware upgrades will be required) and offers forward compatibility with 802.11i. WPA is designed to be a strong, but economical solution for securing enterprise and home WLANs. Before the end of 2003, WPA will be mandatory for Wi-Fi product certification.

Although designed as an interim solution in anticipation of the ratification of 802.11i toward the end of 2003, WPA's strength, economy, and high level of vendor support should ensure its medium- and long-term success in many enterprise environments.

WEP Weaknesses

WEP (Wired Equivalency Privacy), as its name implies, was intended to provide wireless users with the same level of privacy inherent in wired networks. However, after Wi-Fi began to be deployed with some success, researchers in the academic community soon demonstrated that WEP alone did not provide adequate security for wide scale enterprise adoption. Here's a summary of the WEP flaws:

- Weak Keys[1]. This is the most glaring problem with WEP, and RC4 in particular, because it allows an attacker to discover the default key being used by the access point and the client stations, and this in turn enables the attacker to decrypt all messaged being sent over the encrypted channel. There are freely available packages on the Web that allow even casual attackers to discover the WEP key, exploiting this weakness in RC4 (http://sourceforge.net/projects/wepcrack/).
- Initialization Vector (IV) Reuse[2,3,4]. The IV and default key on the station and access point are used to create a key stream, which is in turn used to transform the plaintext message into the WEP encrypted frame. This is depicted in the figure below.

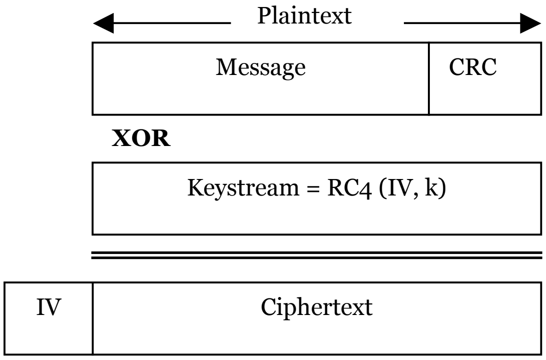


Figure 1: Encrypted WEP frame.

The IV used in WEP is 24 bits long. On a busy network this IV will wrap and be reused. When this is done and the default key (k) has not been changed the security of the network is compromised because the plaintext of messages can be retrieved with reasonable success.

The above flaw allows attackers to retrieve plaintext from messages without knowing the key (k). Statistical analysis of natural languages shows that some characters are used more often than others. So when an e-mail or a text file is being sent over the encrypted channel, the attacker has some clues as to the distribution of characters in the originating plaintext. This coupled with the fact that any two messages using the same IV have can be reduced to the following:

$$C_i = P_i \oplus ks_i$$
$$C_i' = P_i' \oplus ks_i$$

Therefore:

$$C_i \oplus C_i' = Pi \oplus P_i'.$$

Since both ciphertexts are known, the attacker simply tries combinations of P_i and P_i' such that they equal the result of $C_i \oplus C_i'$. This is not too onerous for today's computers and intelligent guesses can be made based on the distribution of characters in natural languages. Moreover, if there is more than one possibility for the plaintext value then the attacker can use the CRC calculated over the plaintext message to arbitrate these possibilities.

- Known plaintext attacks[2,3,4]. This attack also exploits the reuse of the IV in WEP. Keystreams can be determined by sending messages which contain known plaintext over the encrypted channel. Known plaintext often includes the IP and TCP/UDP headers of a message, but it can also include known e-mail messages, which will allow an attacker to determine more of the keystream. Once the keystream is determined, an attacker can forge packets using the same keystream and IV and obtain some access to the protected network.
- Denial of Service attacks. Both 802.1X messages and 802.11 management messages are not authenticated. This makes denial of service attacks trivial to implement.

In short, for most enterprise applications WEP presents too much potential vulnerability for robust, enterprise-wide adoption.

WPA: How It Works

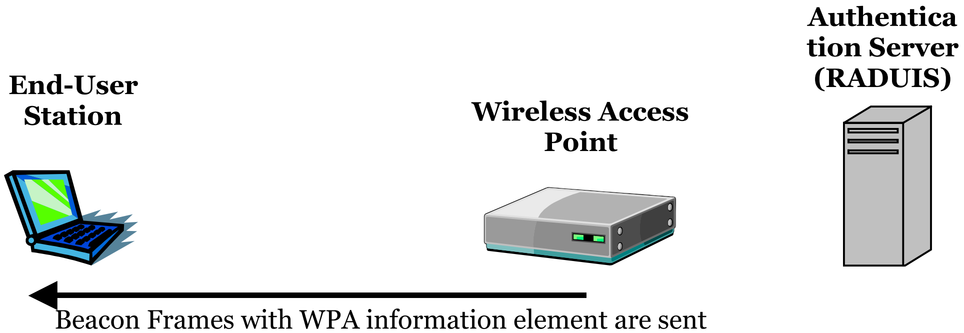
WPA addresses most of WEP's known vulnerabilities and is primarily intended for wireless infrastructure networks as found in the enterprise. This infrastructure includes stations, access points, and authentication servers (typically RADIUS servers). The RADIUS server holds (or has access to) user credentials (e.g., user names and passwords) and authenticates wireless users before they gain access to the network.

WPA's strength comes from an integrated sequence of operations that encompass 802.1X/EAP authentication and sophisticated key management and encryption techniques. Its major operations include:

- Network security capability determination. This occurs at the 802.11 level and is communicated through WPA information elements in Beacon, Probe Response, and (Re) Association Requests. Information in these elements includes the authentication method (802.1X or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES).
- Authentication. EAP over 802.1X is used for authentication. Mutual authentication is gained by choosing an EAP type supporting this feature and is required by WPA. 802.1X port access control prevents full

access to the network until authentication completes. 802.1X EAPOL-Key packets are used by WPA to distribute per-session keys to those stations successfully authenticated.

- Key management. WPA features a robust key generation/management system that integrates the authentication and data privacy functions. Keys are generated after successful authentication and through a subsequent 4-way handshake between the station and Access Point (AP).
- Data Privacy (Encryption). Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.
- Data integrity. TKIP includes a message integrity code (MIC) at the end of each plaintext message to ensure messages are not being spoofed.



Beacon Frames with WPA information element are sent from the AP to the stations in the service set. Information elements include the required authentication method (802.1x or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES). Probe Responses (AP to station) and Association Requests (station to AP) also contain WPA information elements.

Figure 2: WPA Information Element exchange.

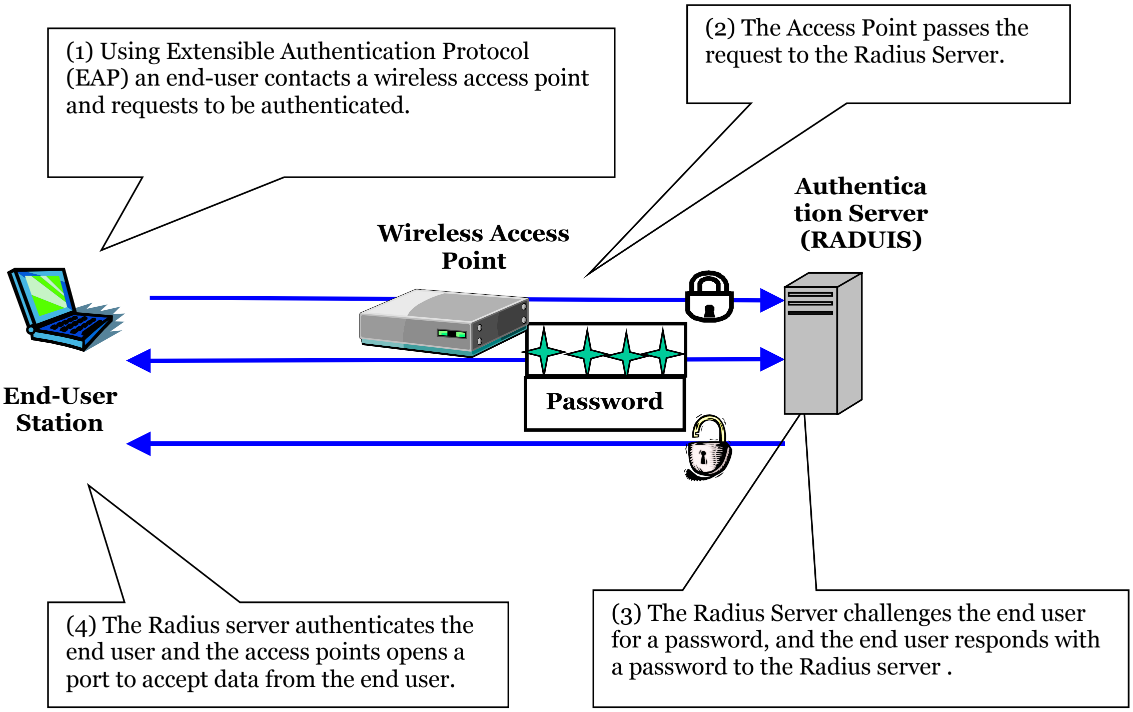
The network capability determination feature is based on changing the 802.11 format of Beacon, Probe Response, and (Re) Association Request frames. As Figure 2 shows, these 802.11 frames now contain network capability information in a WPA information element. The primary information conveyed in the Beacon frames is the authentication method and the cipher suite. Possible authentication methods include 802.1X and Pre-shared key. Pre-shared key is an authentication method that uses a statically configured pass phrase on both the stations and the access point. This obviates the need for an authentication server, which in many home and small office environments will not be available nor desirable. Possible cipher suites include: WEP, TKIP, and AES (Advanced Encryption Standard). We'll talk more TKIP and AES when addressing data privacy below.

The supplicant in the station uses the authentication and cipher suite information contained in the information elements to decide which authentication method and cipher suite to use. For example, if the access point is using the Pre-shared key method then the supplicant need not authenticate using full-blown 802.1X. Rather, the supplicant must simply prove to the access point that it is in possession of the pre-shared key. If the supplicant detects that the service set does not contain a WPA information element then it knows it must use pre-WPA 802.1X authentication and key management in order to access the network.

HOW IT WORKS

802.1X Authentication

The 802.1X standard authenticates wireless LAN end users attempting to access enterprise networks.



(1) Using Extensible Authentication Protocol (EAP) an end-user contacts a wireless access point and requests to be authenticated.

(2) The Access Point passes the request to the Radius Server.

(3) The Radius Server challenges the end user for a password, and the end user responds with a password to the Radius server .

(4) The Radius server authenticates the end user and the access points opens a port to accept data from the end user.

Figure 3: 802.1X Authentication

WPA's authentication process is primarily 802.1X/EAP as shown in Figure 3. (Again, a small office or home environment can opt to deploy the Pre-shared key method). In this mode WPA is restricted to those EAP methods that support mutual authentication of the Supplicant and Authentication Server, such as TLS, TTLS, LEAP and PEAP. Port access control is maintained pending successful authentication by 802.1X.

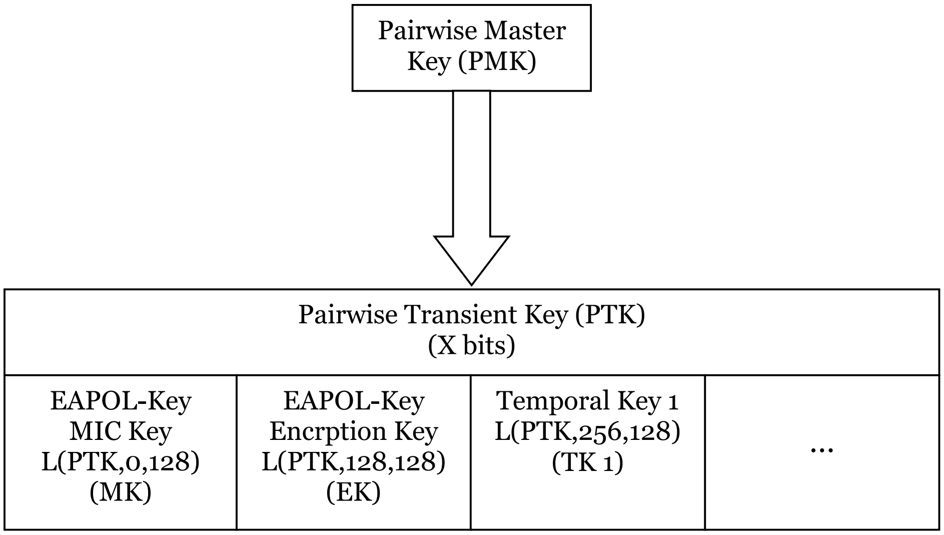

Pairwise Master Key (PMK)
Pairwise Transient Key (PTK) (X bits)
EAPOL-Key MIC Key L(PTK,0,128) (MK)
EAPOL-Key Encrption Key L(PTK,128,128) (EK)
Temporal Key 1 L(PTK,256,128) (TK 1)
...

Figure 4: WPA Key Hierarchy.

As part of the mutual authentication process a Pairwise Master Key (PMK) is generated on the station and RADIUS server, and the RADIUS server sends the PMK to the AP over a secure channel. This is not different than pre-WPA 802.1X authentication. What is different is that the PMK is never used directly with encryption or hashing functions, but instead it is used to generate transient keys which will then be used in the encryption and hash functions. Using transient keys is important because of the weak key attack described earlier. The Pairwise Master Key is never directly involved in generating keystreams for encryption, and this helps thwart any weak key attacks.

Modifications to 802.1X for WPA

Most of the modifications to 802.1X for WPA involve the exchange of EAPOL key descriptors, or packets. This only happens after successful authentication has occurred and does not change the core 802.1X supplicant and authenticator state machines. In WPA, the process of exchanging keys after successful authentication is called the 4-way and Group Key handshakes. The 4-way handshake establishes the pairwise key to be used for unicast traffic while the Group Key handshake establishes and distributes the group key needed for broadcast communication in the service set.

These key state machines are designed to prevent man-in-the-middle and replay attacks. They do this by prescribing the following:

1. The access point's and the station's addresses are used in any 802.1X MIC calculations and validations during the 4-way handshake exchange. This helps bind the key exchange process to a single authenticator and supplicant.
2. Nonces (one time unique values) are used in all 802.1X MIC calculations. This ensures that the keys being used are fresh. That is, new nonces are generated during each 4-way handshake exchange and the value of the pairwise transient key is not only dependent on the pairwise master key but also the supplicant and the authenticator's freshly generated nonce values.
3. The nonces also ensure that neither the station nor the access point is under a replay attack. That is, when nonces are used as part of the key authentication process, the supplicant and authenticator must be in possession of the newly generated PMK, after successful authentication, in order to calculate the required 802.1X MIC values.

There are other subtle changes to 802.1X that make it more compatible with WLANs as opposed to wired switch-based networks for which it was initially designed. First, a PortSecure state value has been added to both the authenticator and supplicant state machines. When this value is true, both the supplicant and the authenticator know that the pairwise and group keys negotiated through the handshake protocols are valid and can be programmed into the NIC's firmware so data traffic can be protected. It is important to synchronize the programming of the keys so both the station and access point are operating in the same mode—secure or in the clear.

Once keys have been programmed into the station's and access point's firmware, any subsequent 802.1X exchange is encrypted. Before WPA, 802.1X exchanges were always done in the clear, and this made the supplicant vulnerable to spoofed EAPOL Logoff messages. (WPA deprecates the use of EAPOL Logoff packets altogether.) This, along with other denial of service attacks using 802.1X, are not longer possible once the encryption keys have been programmed.

Finally, WPA defines an EAPOL MIC error frame. This is an 802.1X key descriptor packet that allows the station to inform the access point when it is under an attack. This packet is sent to the access point when the supplicant receives a MIC error in data frames. If the supplicant receives these packets too frequently then it is under an active attack and counter measures are carried out by the access point, which effectively let's the network administrator know a security problem exists.

TKIP for data privacy

TKIP uses the same RC4 cipher used by WEP, but it adds a variety of techniques to remedy the shortcomings of WEP including a per packet mixing function, a longer initialization vector and a message integrity code (MIC).

TKIP uses a key mixing functions to add another layer of protection against weak key attacks. The key mixing function ensures encryption keys (k from Figure 1) are never used directly as an argument to the RC4 function. In fact, this key mixing function ensures that the encryption key changes on a per packet basis.

To thwart known plain text attacks based on duplicate initialization vectors, TKIP increased the IV size from 24 to 48 bits.

The message integrity hash used in TKIP is known as Michael. It ensures that the contents of data packets have not been sent by another station masquerading as the legitimate station (i.e., the station that has been authenticated and is in possession of the PMK) and that data have not been modified during packet transmission.

Why not AES?

As noted earlier, one of the encryption methods supported by WPA beside TKIP is the advanced encryption standard (AES), although AES support will not be required initially for Wi-Fi certification. This is viewed as the optimal choice for security conscious organizations, but the problem with AES is that it requires a fundamental redesign of the NIC's hardware in both the station and the access point. TKIP was a pragmatic compromise that allows organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

WPA's Likely Success

On the plus side, major 802.11 vendors have announced support for WPA, including Agere, Atheros, Atmel, Colubris, Funk Software, Intersil, Meetinghouse, Proxim, Resonext, and Texas Instruments assuring some level of success.

Given that many overworked network administrators are still playing catch-up regarding their knowledge of WEP, WPA may prove to be a long-term solution for many organizations who will not readily upgrade to the next generation 802.11i solution with AES capability, which requires new hardware on the both the station and access point.

WPA presents a practical answer to dealing with the weaknesses of WEP, based on available technologies and offering forward compatibility with 802.11i and backward compatibility with existing 802.11 solutions. However, WPA does not mandate the advanced encryption standard (AES) for data encryption, deemed the best long term encryption solution for wireless security, and there is still some debate about the best way to smoothly and securely roam from access point to access point in an enterprise environment.

Is It Perfect?

WPA, however, is not without its vulnerabilities. Specifically, it is susceptible to denial of service (DoS) attacks. If the access point receives two data packets that fail the Message Integrity Code (MIC) check within 60 seconds of each other then the network is under an active attack, and as a result, the access point employs counter measures, which includes disassociating each station using the access point. This prevents an attacker from gleaning information about the encryption key and alerts administrators, but it also causes users to lose network connectivity for 60 seconds.

More than anything else, this may just prove that no single security tactic is completely invulnerable. WPA is a definite step forward in WLAN security over WEP and has to be thought of as a single part of an end-to-end network security strategy.

About the Meetinghouse AEGIS WPA Solution

Meetinghouse announced its support for WPA in April 2003. AEGIS Client and Server are differentiated from other WLAN security solutions in the breadth of EAP methods and operating system supported. AEGIS Client supports EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, and Cisco's LEAP on Linux, Mac OS X , Windows XP, NT, 2000, 98, ME, and Pocket PC 2002. AEGIS Server supports MD5, TLS, TTLS, LEAP and PEAP on Linux, Solaris, and Windows XP/2000.

Meetinghouse also provides 802.1X, RADIUS, and WPA protocol stacks designed to integrate into existing APs. These stacks have been written with portability in mind and they run on various real-time operating systems including Linux, VxWorks, and Nucleus.

AEGIS provides secure WPA-compatible authentication for wireless LANs in enterprise and public access networks. AEGIS provides the enhanced tunneling authentication solutions, TTLS and PEAP. Tunneled authentication simplifies network management, eliminates the burden of client-side certificates, and leverages existing standard user name and password infrastructure. AEGIS Client and AEGIS Server software can be used with other industry standard 802.1X and WPA solutions.

Summary

WPA, plus other advancements such as tunneled EAP methods, enables a strong, practical solution to enterprise-class Wireless LAN security utilizing already deployed hardware. Backward compatibility protects 802.11 legacy solutions from obsolescence, an important consideration in today's resource constrained IT organizations. Forward compatibility protects the enterprise as it migrates to the next phase of WLAN security, 802.11i (WPA2) in the longer term.

References

1. S. Fluhrer, I. Mantin, and A. Shamir. *Weaknesses in the Key Scheduling Algorithm of RC4*. Unpublished.
2. J. Walker. *Unsafe at any key size; An analysis of the WEP encapsulation*. IEEE Submission, October, 2000.
3. N. Borisov, I. Goldberg, D. Wagner. *Intercepting Mobile Communications: The Insecurity of 802.11*. Unpublished.
4. W. Arbaugh, N. Shankar, and Y.C. Wan. *Your 802.11 Wireless Network has No Clothes*. March 30, 2001.