Buy, Sell or Hold – is WPA the Answer to Secure Enterprise WLANS
GIAC Security Essentials Certification (GSEC)
Version 1.4b
Option 1
By Michael Leonard
April 26, 2004

Abstract

With the ratification of 802.11i still looming in the future has the 'pre release' of Wi-Fi Protected Access (WPA) ushered in the era of secure wireless networking?

Wireless networking is without a doubt one of the fastest growing and most exciting segments within the technology arena and Network Administrators and Data Security experts everywhere are evaluating its promise. The much-heralded weaknesses of WEP have not put a damper on the explosive growth of this technology, especially in the home and small office environment. But, are the security enhancements introduced with the WPA standard sufficient for safe deployment of wireless networks (WLANS) in a corporate environment?

The purpose of this paper is to briefly review the known deficiencies of WEP then examine the security enhancements available in WPA and the forthcoming 802.11i standard and conclude if WPA is ready for the enterprise environment, or if we must wait until the full ratification of the 802.11i standard.

WPA defined

The Institute of Electrical and Electronic Engineers (IEEE) released the 802.11 standard in 1997. This standard describes Wireless Local Area Networks (WLAN) and provides a security mechanism known as Wired Equivalent Privacy (WEP). The security capabilities of WEP were soon called into question and by 2001 WEPs cryptographic deficiencies had become well documented. [1] With the explosive growth of Wireless LAN technologies the industry needed a secure replacement for WEP.

WPA is the first standards based attempt at answering WEPs shortcomings, even though many vendors provided third party solutions. WPA is a pre-release of much of the security enhancements that will be included in the full 802.11i standard that is scheduled for ratification in June of 2004. WPA was made available early to help fill the security gap and to help an industry that would otherwise suffer from the tarnished image created by WEP. In a nutshell, WPA offers better encryption, data authenticity and user authentication. WPA addresses the security triad of Confidentiality, Integrity and Availability.

The WPA standard was designed to function with all flavors of 802.11 (a, b & g). WPA is also intended to be a software release that should be compatible with most newer enterprise class Access Points and wireless network cards (whether this is accurate is outside the scope of this paper). It, therefore, should be an inexpensive upgrade since all that is required is a firmware upgrade to the Access Point and network interface card (NIC). It promises to be forward compatible with the 802.11i, often referred to as WPA2, but WPA capable hardware is not guaranteed to be capable of running WPA2 due to WPA2's use of the Advanced Encryption Standard (AES) algorithm. AES will require more sophisticated hardware on the Access Point and NIC.

WPA was designed to improve security for both the Small Office Home Office (SOHO) user as well as within the enterprise environment. It does so by providing two modes, Corporate and Pre Shared Key (PSK). The former requires authentication services, usually via Remote Authentication Dial-In User Service (RADIUS), which would not normally exist in the small office or home environment.

WPA is touted as an interim fix that addresses the security flaws in the WEP standard while allowing enterprises to extend their investment in wireless hardware in anticipation of the ratification of 802.11i. WPA has widespread support throughout the industry. Companies such as Microsoft, Intel, Proxim and Agere have announced support for this technology.

Wireless Threats

In addition to the common threats that all networks are susceptible to wireless networks have additional threat vectors that administrators and security professionals must be cognizant of. Due to the very nature of a wireless connection, passing data through the air on radio waves, it is difficult and costly to contain the wireless frequencies. Shielding buildings and utilizing directional antennas can reduce these problems but these countermeasures are difficult and cost prohibitive.

The most common threats that affect the wireless network are: [7]

- Eavesdropping (passive and active) – the casual passerby or hacker just needs to be within radio range to begin intercepting data. Confidentiality is compromised.
- Session Hijacking – by intercepting the login confirmation the intruder tricks the network in to thinking a legitimate user is being granted network access. Integrity is compromised.
- Denial of Service – Wireless Access Points can be flooded relatively easily making it unavailable for legitimate use. Availability is compromised.
- Theft of Bandwidth – an unprotected Wireless Access Point is an opportunity for an intruder to receive access to the Internet or worse, the internal network.

- Spoofing – An intruder can install a rogue Wireless Access Point and allow clients to connect. Once connected it is possible for the intruder to gather sensitive data from the client.

The range of a wireless network is typically thought to be limited to several hundred feet but an intruder with the proper equipment will be able to tap into signals at great distances.

It's important to note that these threats can apply in the absence of a Wireless Access Point. A laptop or desktop computer with a wireless network card installed and configured to accept ad-hoc wireless connections is another point of entry for an intruder. The intruder need only come into proximity of the ad-hoc network and can then begin probing for access.

WEP deficiencies

The intent of this paper is not to discuss WEP in detail but a brief overview is necessary to provide a backdrop for WPA. The flaws within the WEP standard are widely known and documented. Specifically WEP suffers from a poor implementation of the RC4 algorithm and weak user authentication capabilities. The RC4 algorithm itself is not at fault, in fact, RC4 is used everyday in SSL to provide secure online transactions. Instead, it is mistakes in the implementation of RC4 that makes WEP insecure. Automated tools can crack WEP's encryption key with as little as 100mb of data captured from the air – a trivial task with freely available tools.[2]

Let's first examine the Authentication process that WEP employs. WEP utilizes a Service Set Identifier (SSID) that must be known to both the client and the Access Point in order for the client to attach, but the SSID is passed in the clear so it is easy to determine an Access Point's SSID utilizing a protocol analyzer and wireless NIC. Its possible to lower this risk, if only by a little, by turning off SSID broadcasts but this is not sufficient to provide a reasonable level of security. In addition to knowing the SSID, an intruder must also correctly respond to a *Challenge* issued by the Access Point. The Access Point encrypts a random piece of data and sends it to the client. The client must decipher the string and pass back the original string as plain text to the Access Point. Unfortunately, an intruder needs only capture this conversation to be able to decipher all future challenges. [3]

WEP has very weak data integrity protection mechanisms. An attacker can make changes to data in a captured packet while not effecting the packet's checksum, thereby circumventing WEPs CRC based integrity check.

MAC address filtering is offered by some vendors as a method of only permitting authorized devices onto the network, but since MAC addresses are passed in the clear it is again trivial to capture this data and then masquerade as an authorized client. MAC address filtering is only effective in keeping out the causal passer-by but completely ineffective against a targeted attack.

There are freely available tools that will allow an intruder to carry out all of these attacks with little more than a laptop with a wireless network card. One of the most popular is AirSnort. Once an intruder has captured enough data access to the network is assured.

There are 'bolt-on' measures that can be deployed to mitigate these weaknesses. VPN, Firewalls and 802.1x authentication can all be implemented to alleviate the aforementioned risks. In the end they are just workarounds to a fundamentally flawed standard.

WPA - Wi-Fi Protected Access

How does WPA provide better security? It does so by providing strong encryption, proven authentication via 802.1x/EAP and an enhanced integrity checking mechanism. WPA was thoroughly tested by well-known cryptographers and promises to provide true *Wired Equivalent Privacy*. And, since it can be run on today's hardware it is an attractive upgrade.

Enhanced Authentication

802.11i (and WPA) require stronger authentication – this function is not optional. WPA provides mutual authentication of the client and Access Point through 802.1x and one of the Extensible Authentication Protocol (EAP) types. This ensures that the network knows the client and also, just as importantly, that the client is connecting to an authorized Access Point and not a rogue device installed by an intruder. 802.1x is an IEEE standard that provides port-based security for wired and wireless networks alike. One of the strengths of EAP is its versatility. EAP allows an administrator to verify user credentials in several ways including username and password, certificate-based authentication, secure ID's, etc.

As stated earlier WPA allows for two modes of operation, Corporate and Pre Shared Key (PSK). The following will focus on the Corporate Mode with an authentication infrastructure in this case a RADIUS server.

Let us look at the conversation that takes places when a wireless client attempts to associate with an access point in an environment with a RADIUS server:

1. The Supplicant (802.1x terminology for client) attempts to associate with an access point by requesting to be authenticated.
2. The Authenticator (802.1x terminology for the Access Point or switch) challenges the Supplicant for an EAP identity request.

3. The Authenticator passes the Supplicants response to an Authentication Server (commonly a RADIUS server).
4. The Authentication Server issues an Authentication Challenge that is passed to the Supplicant via the Authenticator.
5. The supplicant responds via the Authenticator and if accepted by the Authentication Server is permitted onto the network.

802.1x/EAP provides the ability to authenticate users at the point of entry and effectively keeps intruders from accessing the network. By requiring layer 2 access control WPA represents a big step forward in security.

802.1x/EAP's versatility goes further by providing several EAP types to choose from, including:

- EAP-MD5
- EAP-SecureID
- Lightweight Extensible Authentication Protocol (LEAP)
- Protected Extensible Authentication Protocol (PEAP)
- EAP-Transport Layer Security (EAP-TLS)
- EAP-Tunnel Transport Layer Security (EAP-TTLS)

Other types exist and the list will continue to grow. The WPA standard supports many EAP types, however it does not prescribe any particular one.

Choosing an EAP type depends on the level of security required and how well it integrates into a given computing environment. One's existing infrastructure will have an impact on the EAP type one would ultimately select. Cost can also be a factor if two-factor authentication is required. WPA mandates the use those EAP types that provide mutual authentication. [4]

MD5 – Although it is easy to implement and widely supported it does not support mutual authentication and is exploitable via a dictionary attack (this risk can be reduced through use of strong passwords). MD5 should not be used in an environment where strong security is necessary. Because it lacks mutual authentication it is not supported in WPA.

EAP-SecureID – Although it does not provide mutual authentication it is by its nature a two factor authentication method. It provides tunneled authentication.

EAP-LEAP – Proprietary solution developed by Cisco. Susceptible to dictionary attacks. Supports mutual authentication.

EAP-PEAP – Client authentication is protected within an encrypted tunnel. It can be considered strong authentication. Supports mutual authentication.

EAP-TLS – Strong security is achieved via this certificate based system. It requires a PKI infrastructure rather than user IDs and passwords. Supports many client platforms. It can be considered strong authentication but also potentially the most costly. Supports mutual authentication.

EAP-TTLS – Like PEAP, TTLS utilizes an encrypted tunnel to pass authentication data. It is considered strong authentication and is compatible with older authentication methods (PAP, CHAP, CHAPv2). Requires a proprietary client. Supports mutual authentication.

Again, the EAP type you select will be based largely on one's security requirements and existing computing infrastructure.

For the home and small office environment where an authentication infrastructure is not practical WPA offers Pre Shared Key mode. Pre Shared Key is essentially a password that is entered on the Access Point and on each client. Pre Shared Key mode utilizes the Temporal Key Integrity Protocol (TKIP) and MIC and can be considered secure for this type of environment.

Pre Shared Key is not appropriate for widespread use in an enterprise environment. One issue is its susceptibility to a dictionary attack. This risk can be reduced, however by choosing a strong shared secret. A second issue is its lack of scale, it would be impractical to change the shared secret of every Access Point and client if the shared secret were to be compromised.

Better Encryption

The *key* to better security is in the *key*. Whereas WEP used a static key for all clients and Access Points WPA employs a dynamic per session, per user, per packet key rotation scheme making it exponentially more difficult for an intruder to exploit.

This enhanced encryption is achieved through the use of the Temporal Key Integrity Protocol (TKIP). Once the user has associated with the Access Point, TKIP manages the encryption scheme that will be utilized during the session. The unique master key that was generated during the authentication process will act as the starting point for all subsequent packets. TKIP passed this master key to the Access Point and the client and coordinates the key rotation for the duration of the session. [1] Unicast traffic is protected by the Pairwise Transient Key which is derived from the Pairwise Master Key. The Groupwise Transient Key protects multicast traffic.[10]

TKIP utilizes a process called the Message Integrity Check (MIC) to ensure that the Access Point receives the same data that the client sent. By placing an 8 byte code between the data and Integrity Check Value then encrypting it along with the data payload MIC ensures data integrity. MIC is also responsible for defeating replay attacks by managing a frame counter field new to 802.11.

The security enhancements available in the WPA standard are without question more robust then the predecessor WEP standard. WPA increases the key size from 40 bits to 128. It increases the number of keys in use from one with WEP to 500 trillion in WPA. These improvements c oupled with MIC's enhanced integrity checking mechanism make intrusion a significantly more difficult task. WPA has not been cracked and can be considered a viable option for safe wireless networking.

What's Next? 802.11i (WPA2)

WPA makes available today most of the security enhancements that will be integrated in the 802.11i (WPA2) standard. WPA2 goes further by incorporating the Advanced Encryption Standard (AES) as its cipher engine. The U.S. Department of Commerce and the National Institute of Standards and Technology have approved AES.

This increased encryption strength will come at a cost, namely, hardware. Unlike WPA, deployment of WPA2/AES will likely require new Access points not just software upgrades. Hence, the dilemma for entities that want to deploy WLANS – wait for approval of 802.11i or roll the dice and purchase "802.11i Upgradeable" devices.

WPA2 will not be ratified until mid 2004 and it will be several months after that until widespread certified product availability. WPA2 will also support Ad-Hoc mode.

AES

AES is a symmetric, block cipher with variable key lengths of 128, 192 or 256. The increased key length means that using today's technology it would take 149 trillion years to crack. Even in an age where IT budgets are constrained, AES should outlive even the stingiest IT budgets.

AES holds great promise as an encryption mechanism with strong security yet capable of encrypting and decrypting data much faster than its predecessors with little resource consumption. AES is based on the Rijndael algorithm. Rijndael is named after its developers Vincent Rijmen and Joan Daemen. [5] AES was selected by the National Institute of Standards and Technology to supplant DES.

Interoperability Issues

The interoperability issue is two-fold, hardware and authentication method. The hardware issue results from vendors trying to jump the gun and release hardware today that is upgradeable to the new requirements of 802.11i (AES), but until the standard is ratified it will be difficult for vendors to guarantee future compatibility. IT departments must be certain that their investment in 802.11i is protected, or be forced to wait for full ratification and the production of certified products. [9]

TruSecure's ICSA Laboratory and the Wi-Fi Alliance are two organizations that intend to conduct cross vendor interoperability testing as these products enter the marketplace.[9]

The authentication issue promises to be just as complicated, maybe more. In 2002 Cisco and Microsoft set out to create the Protected Extensible Authentication Protocol [8] as a method for secure authentication that does not require certificates in the wireless environment. Unfortunately the two companies are now split on PEAP, and both offer versions that are incompatible with the other. Cisco's PEAP client will not be capable of authenticating to a Microsoft back end and the same can be said for Microsoft's PEAP client, which can't authenticate with Cisco. There is no indication that the two companies will reach agreement.

WPA and the Remote User

Utilizing WPA in the enterprise environment will not prohibit users from connecting to public (open) hot spots where WPA is not in use. These hotspots operate in Open mode where neither encryption nor authentication is in place.

Of course, a secure connection back to the enterprise network needs to be achieved via a VPN including personal firewall software on the laptop to protect data communications.[6]

Conclusion

The security advances introduced in WPA fix the shortcomings of WEP. WPA gives IT departments the assurance that only authorized clients are connecting to their networks. It ensures that data is kept private from prying eyes, and guarantees that the data transmitted is the same as the data received. In doing so, WPA addresses the security triad on Confidentiality, Integrity and Availability.

If your enterprise has deployed WEP and "bolted-on" security via Firewalls, 802.1X, IPSEC VPN, etc it may pay to wait for the full ratification of 802.11i. You will preserve and extend your investment in these technologies. However, if your WEP based Access Points are upgradeable to WPA you should strongly consider deploying it. WPA will provide good security for your environment and will be forward compatible with the 802.11i standard.

For enterprises that have deployed WEP and are relying on its security mechanisms you should upgrade to WPA immediately, provided your hardware allows, or remove these devices from service.

For enterprises that have deployed WPA there may not be a need to jump directly to WPA2 when it becomes available. Wireless hardware will undoubtedly change drastically over the upcoming years and your WPA deployment is considered secure. You will be able to protect this investment and wait until the 802.11i standard is released and hardware is made available and tested in the enterprise environment.

References

[1] Wi-Fi Alliance. “Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks” 29 April 2003 URL: http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf

[2] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK USA:SANS Press, February 2003. P61

[3] Steinke, Steve. “Security and 802.11 Wireless Networks” 05 June 2002 URL: http://www.networkmagazine.com/article/NMG20020603S0011

[4] Burns, Jim. “Selecting an Appropriate EAP Method for Your Wireless LAN” 01 February 2003 URL: http://www.mtghouse.com/MDC_EAP_White_Paper.pdf

[5] Network World Fusion. AES (Advanced Encryption Standard) http://www.nwfusion.com/details/597.html

[6] Wi-Fi Alliance, “Enterprise Solutions for Wireless LAN Security” 06 February 2003 URL: http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Enterprise2-6-03.pdf

[7] The Canadian Institute of Chartered Accountants, “Security for Wireless Systems” 1 February 2004 URL: http://www.cica.ca/multimedia/Download_Library/Standards/Studies/English/ITAC-wireless-e.pdf

[8] Messmer, Ellen “Microsoft, Cisco Prepare for PEAP Show” 23 September 2002 URL: http://www.nwfusion.com/news/2002/0923peap.html

[9] Messmer, Ellen “Wireless LAN Worries” 12 January 2004 URL: http://www.nwfusion.com/news/2004/0112wlansecurity.html

[10] Butti, Laurent. Veysset, Franck. “Wi-Fi Security: What’s Next?” September 2003 URL: http://www.toorcon.org/slides/80211security/toorcon03-0.1.pdf P23-25