Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)

Paul Arana
INFS 612 – Fall 2006

Abstract

With the increase in use of Wireless Networks, the initial protocols, Wireless Equivalent Privacy (WEP) first, then Wi-Fi Protected Access (WPA), used to secure wireless communications were found inadequate due to many proven vulnerabilities so a new protocol was implemented, the Wi-Fi Protected Access 2 (WPA2) protocol. This paper will first discuss the benefits of the Wi-Fi Protected Access 2 (WPA2) protocol used to secure communications in Wireless Networks over previous protocols and the vulnerabilities addressed by it, then it will discuss the available modes to secure a wireless network using the Wi-Fi Protected Access 2 (WPA2) protocol and finally explore its vulnerabilities. In conclusion, this paper will present possible solutions and/or suggestions on how the Wi-Fi Protected Access 2 (WPA2) protocol vulnerabilities might be mitigated and/or addressed through enhancements or new protocols.

1. Introduction

The IEEE 802.11i standard also known as Wi-Fi Protected Access 2 (WPA2) is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. The draft standard was ratified on June 24th, 2004, and replaces the previous security specifications, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced as an intermediate solution to WEP insecurities. WPA implemented only a subset of IEEE 802.11i. WPA2 makes use of a specific mode of the Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) protocol (CCMP). CCMP provides both data confidentiality (encryption) and data integrity. The use of the Advanced Encryption Standard (AES) is a more secure alternative to the RC4 stream cipher used by WEP and WPA.

2. WPA2

The WPA2 standard has two components, encryption and authentication which are crucial to a secure wireless LAN. The encryption piece of WPA2 mandates the use of AES (Advanced Encryption Standard) but TKIP (Temporal Key Integrity Protocol) is available for backward compatibility with existing WAP hardware. The authentication piece of WPA2 has two modes: Personal and Enterprise. The Personal mode requires the use of a PSK (Pre-Shared Key) and does not require users to be separately authenticated. The Enterprise mode, which requires the users to be separately authenticated based on the IEEE 802.1X authentication standard, uses the Extended EAP (Extensible Authentication Protocol) which offers five EAP standards to choose from: EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), Protected EAP vo/EAP-Microsoft's Challenge Handshake Authentication Protocol v2 (PEAPvo/EAP-MSCHAPv2), Protected EAP v1/EAP-Generic Token Card (PEAPv1/EAP-GTC) and EAP-Subscriber Identity Module of the Global System of Mobile Communications (EAP-SIM). The Enterprise mode has the following hardware/software implementation requirements:

- Selection of EAP types that will be supported on stations, APs (Access Point), and authentication servers.
- Selection and deployment of authentication servers typically RADIUS (Remote Authentication Dial In User Service) based authentication servers.
- WPA2 software upgrades for APs and clients.

WPA2 establishes a secure communication context in four phases. In the first phase the parties, AP and the client, will agree on the security policy (authentication method, protocol for unicast traffic, protocol for multicast traffic and pre-authentication method) to use that is supported by the AP and the client. In the second phase (applicable to Enterprise mode only)

802.1X authentication is initiated between the AP and the client using the preferred authentication method to generate an MK (common Master Key). In the third phase after a successful authentication, temporary keys (each key has limited lifetime) are created and regularly updated; the overall goal of this phase is key generation and exchange. In the fourth phase all the previously generated keys are used by the CCMP protocol to provide data confidentiality and integrity.

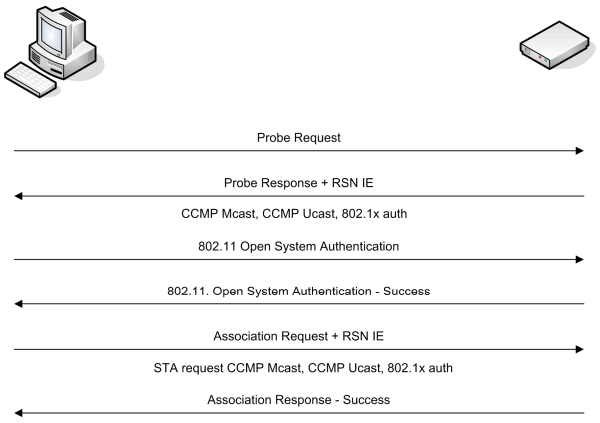

Figure 1. Agreeing on the security policy

2.1. WPA2 Authentication

One of the major changes introduced with the WPA2 standard is the separation of user authentication from the enforcement of message integrity and privacy, thereby providing a more scalable and robust security architecture suitable to home networks or corporate networks with equal prowess.

Authentication in the WPA2 Personal mode, which does not require an authentication server, is performed between the client and the AP generating a 256-bit PSK from a plain-text pass phrase (from 8 to 63 characters). The PSK in conjunction with the Service Set Identifier and SSID length form the mathematical basis for the PMK (Pair-wise Master Key) to be used later in key generation.

Authentication in the WPA2 Enterprise mode relies on the IEEE 802.1X authentication standard. The major components are the supplicant (client) joining the network, the authenticator (the AP serves as the authenticator) providing access control and the authentication server (RADIUS) making authorization decisions. The authenticator (AP) divides each virtual port into two logical ports, one for service and the other for authentication, making up the PAE (Port Access Entity). The authentication PAE is always open to allow authentication frames through, while the service PAE is only open upon successful authentication by the RADIUS server. The supplicant and the authenticator communicate using Layer 2 EAPoL (EAP over LAN). The authenticator converts EAPoL messages to RADIUS messages and then forwards them to the RADIUS server. The authentication server (RADIUS), which must be compatible with the supplicant's EAP types, receives and processes the authentication request. Once the authentication process is complete the supplicant and authenticator have a secret MK (Master Key) as shown in Figure 2.

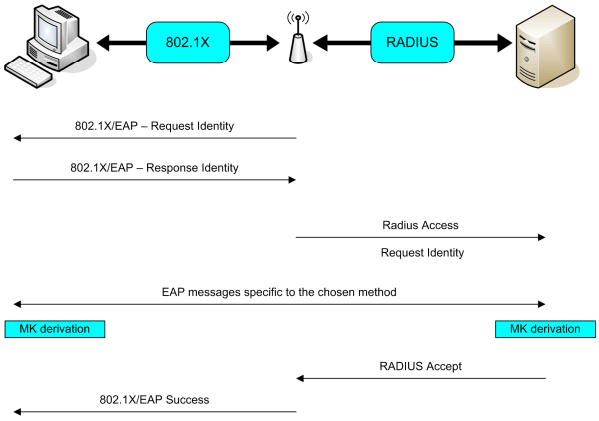

Figure 2. 802.1X authentication [5]

2.1. WPA2 Key generation

WPA2 key generation is accomplished by means of two handshakes: a *4-Way Handshake* for PTK (Pair-wise Transient Key) and GTK (Group Transient Key) derivation, and a *Group Key Handshake* for GTK renewal.

The *4-Way Handshake*, accomplished by four EAPoL-Key messages between the client and the AP, is initiated by the access point and performs the following tasks:

- Confirm the client's knowledge of the PMK. The PMK derivation, required to generate the PTK, is dependent on the authentication

method used. In WPA2 Personal mode the PMK is derived from the authentication PSK and for WPA2 Enterprise mode the PMK is derived from the authentication MK (key hierarchy in Figure 3).

- Derive a fresh PTK, which is comprised of three types of keys: KCK (Key Confirmation Key – 128 bits) used to check the integrity of EAPoL-Key frames, KEK (Key Encryption Key – 128 bits) used to encrypt the GTK and the TK (Temporal Keys – 128 bits) used to secure data traffic.
- Install encryption and integrity keys.
- Encrypt transport of the GTK which is calculated by the AP from a random GMK (Group Master Key).
- Confirm the cipher suite selection

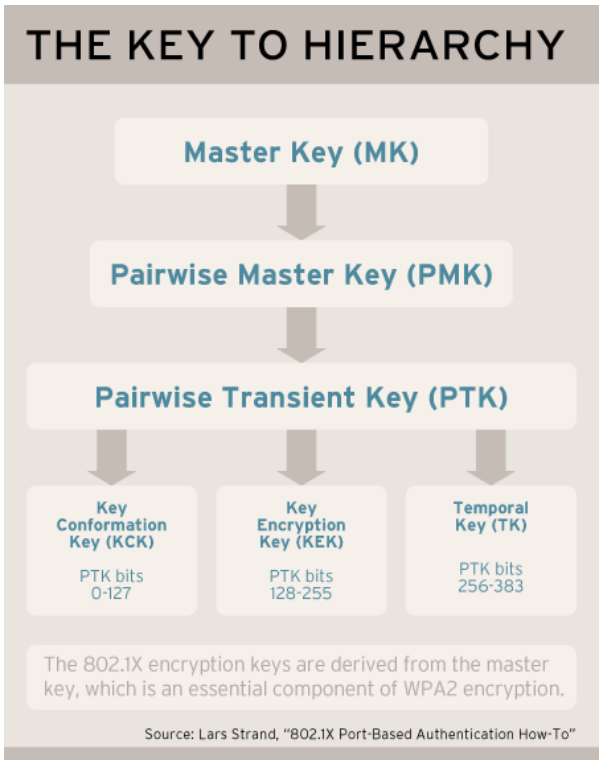

Figure 3. MK hierarchy [7] [14]

The *Group Key Handshake* is only used to disassociate a host or renew the GTK and uses the KEK generated during the *4-Way Handshake* to encrypt the GTK.

2.2. WPA2 Encryption

The AES used by WPA2 "is a block cipher, a type of symmetric key cipher that uses groups of bits of a fixed length – called blocks" [4]. A symmetric key cipher is a set of instructions or algorithm that uses the same key for both encryption and decryption. In the WPA2/802.11.i implementation of AES, bits are encrypted (using a 128 bit key length) in blocks of plaintext, that are calculated independently, rather than a key stream acting across a plaintext data input stream. AES encryption includes 4 stages that make up one round and each round is iterated 10 times.

AES uses the Counter-Mode/CBC-Mac Protocol (CCMP). CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication (with different initialization vectors). The two underlying modes employed in CCM include Counter mode (CTR) , shown in Figure 4, that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.

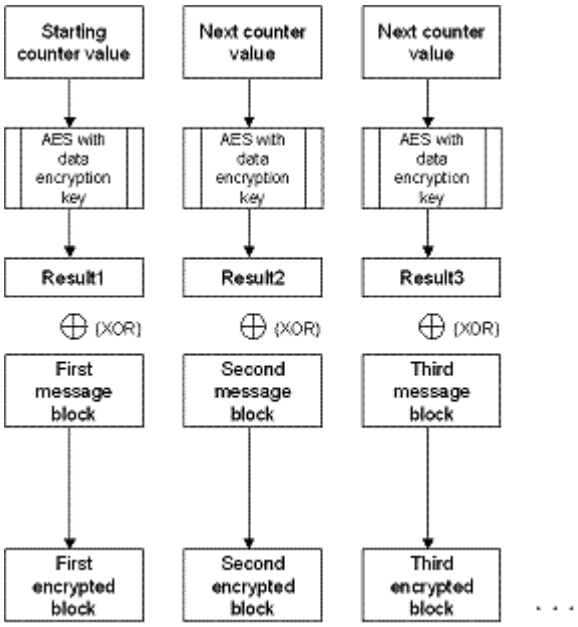

Figure 4. AES Counter Mode [2]

CBC-MAC is used to generate an authentication component as a result of the encryption process (Figure 5). This is different from prior Message Integrity Code (MIC) implementations, in which a separate algorithm for integrity check is required. To further enhance its advanced encryption capabilities, AES uses a 128-bit Initialization Vector (IV).

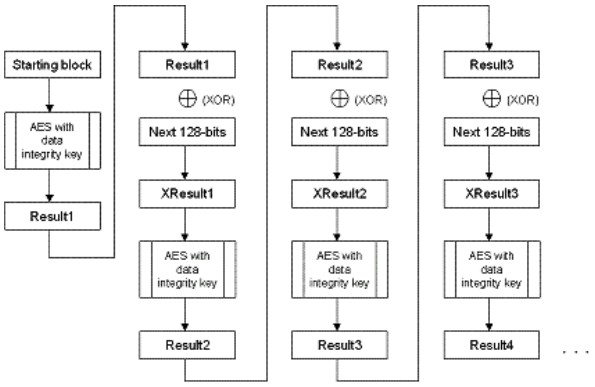

Figure 5. AES CBC-MAC [2]

2.2.1 WPA2 Encryption Steps

The MIC - similar to a checksum - provides data integrity for the nonchangeable fields in the 802.11 header, unlike WEP and WPA, preventing packet replay from being exploited to decrypt the package or compromise cryptographic information. The MIC is calculated using a 128-bit IV as follows:

1. IV is encrypted with AES and TK to produce a 128-bit result.
2. 128-bit result is XOR with the next 128 bits of data.
3. The result of XOR is then passed through steps 1 and 2 until all 128 blocks in the 802.11 payload are exhausted.
4. At the end of the operation the first 64 bits are used to produce the MIC.

The Counter Mode algorithm encrypts the data and the MIC (calculated using the CBC-MAC). The Counter Mode algorithm begins with a 128-bit counter preload similar to the MIC IV, but uses a counter value initialized to 1 instead of a data length resulting in a different counter used to encrypt each packet. The data and the MIC are encrypted as follows:

1. Initialize counter if it is the first time otherwise increment counter.
2. First 128 bits are encrypted using AES and TK to produce a 128-bit result.
3. A XOR is performed on the result of step 1.
4. The first 128 bits of data produce the first 128-bit encrypted block.
5. Repeat steps 1-4 until all the 128-bit blocks have been encrypted.
6. Set counter to zero and encrypt it using AES and XOR with MIC appending the result the encrypted frame.

2.2.2 WPA2 Decryption Steps

Decryption works in reverse. Here are the summarized steps:

1. Using the same algorithm for encryption the counter value is derived.
2. The value from step 1 and the encrypted portion of the 802.11 payload are decrypted using the Counter Mode algorithm and TK. The result is the MIC and decrypted data.
3. The date then is processed by the CBC-MAC algorithm to recalculate the MIC and the values from step 3 and 2 do not match the packet is dropped. Otherwise, the decrypted data is sent up to the network stack and to the client.

3. Benefits of WPA2

WPA2 (along with WPA) resolved vulnerabilities of WEP to "hacker attacks such as 'man-in-the-middle', authentication forging, replay, key collision, weak keys, packet forging, and 'brute–force/dictionary' attacks"[4]. By using government grade AES encryption and 802.1X/EAP authentication WPA2 further enhances the improvements of WPA using TKIP encryption and 802.1X/EAP authentication over WEP's imperfect encryption key implementation and its lack of authentication. "AES has no known attacks and the current analysis indicates that it takes 2^{120} operations to break an AES key" [4].

In addition to the encryption benefits, WPA2 also adds two enhancements to support fast roaming of wireless clients moving between wireless AP's.

- PMK caching support – allows for reconnections to AP's that the client has recently been connected without the need to re-authenticate.

- Pre-authentication support – allows a client to pre-authenticate with an AP towards which it is moving while still maintaining a connection to the AP it's moving away from.

PMK caching support and Pre-authentication support enable WPA2 to reduce the roaming time from over a second to less than $1/10^{th}$ of a second. The ultimate benefit of the fast roaming is that WPA2 can now support timing-sensitive applications like Citrix,

video, or VoiP (Voice over IP) which would break without it.

4. Vulnerabilities of WPA2

DoS (Denial of Service) attacks like RF jamming, data flooding, and Layer 2 session hijacking, are all attacks against availability. None of the Wi-Fi security standards can prevent attacks on the physical layer simply because they operate on Layer 2 an above. Similarly none of the standards can deal with AP failure.

Management Frames – report network topology and modify client behavior - are not protected so they provide an attacker the means to discover the layout of the network, pinpoint the location of devices therefore allowing for more successful DoS attacks against a network.

Control Frames – are not protected leaving them open to DoS attacks.

Deauthentication – the aim is to force the client to reauthenticate, which coupled with the lack of authentication for control frames which are used for authentication and association make it possible for the attacker to spoof MAC addresses (for more details refer to [7][15]) . Mass deauthentication is also possible.

Disassociation – the aim is to force an authenticated client with multiple AP's to disassociate from them therefore affecting the forwarding of packets to and from the client (for more details refer to [15]).

5. Solutions

Centrally managed thin access points that can communicate with one another help secure information related to roaming clients and will improve availability by dynamically adjusting the RF power level. Operational security measures such as site surveillance, as well as planning the Wi-Fi RF coverage area, can also improve availability by reducing the risk of attacks like RF jamming.

There is an initiative called IEEE 802.1w Task Group (TG) that was approved in March 2005. The main goal of this task group is to improve the security of wireless networks by protecting management frames. The solution will be able to identify spoofed management frames and disregard malicious traffic normally used to launch DoS attacks against the network, such as a deauthenticate flood attack. The estimated date for the IEEE 802.11w (shown in Figure 6) specification is April 2008 so it's possible that the mechanisms adopted by the working group could change drastically. The IEEE 802.1w TG has not indicated that it intends to extend the protection to control frames on the wireless network.

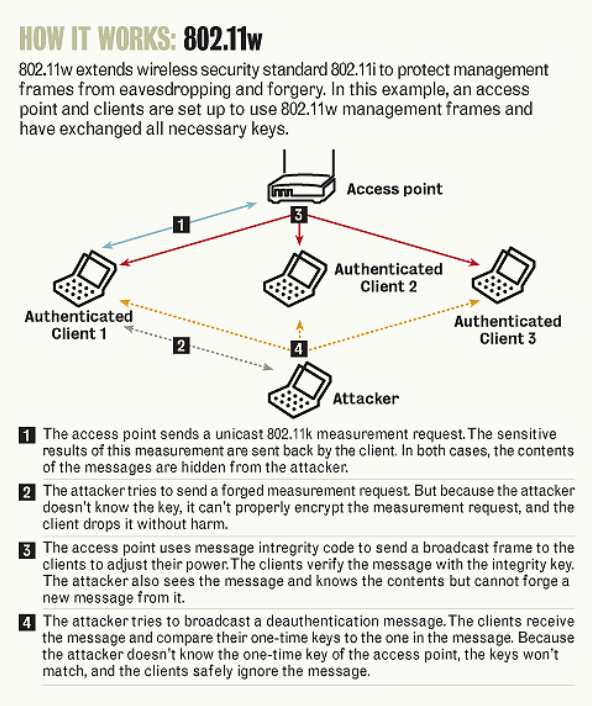

Figure 6 IEEE 802.11W

The proposed IEEE 802.11w will provide three types of protection. The first is for unicast management frames – used to report network topology and modifying client behavior- and it will achieved by extending the AES encryption to these frames to protect them from forgeries while providing confidentiality. The second is for generic broadcast management frames – used to adjust radio frequency properties or start measurements – and it will achieved by appending a MIC (message integrity code) to the non-secure frame protecting them from forgeries but not confidentiality since this frames do not carry sensitive information. The third one is for deauthentication and disassociation frames to be accomplished by using a pair of related one-time keys (a secret one for the AP and the other one for the client) which will allow the client to determine if the deauthentication is valid.

6. Conclusion

In conclusion, there are some procedures to mitigate the RF jamming, and the future specification IEEE 802.11 W will extend the protection to management frame effecting a reduction in the opportunities to launch DoS attacks. I hope that the IEEE 802.11 TG will consider including the control frames in the specification will then eliminate most the vulnerabilities of wireless networks using WPA2/IEEE 802.11X.

Finally a solution that will not resolve the deficiencies of the WPA2 standard but can greatly improve overall security would be to require all wireless networks to be upgraded to the IEEE 802.11i/WPA2 standard since the majority of wireless networks are not WPA2 compliant. The benefits of having all wireless networks conform to the latest standard will outweigh the cost and logistics of upgrading and will ultimately provide a much greater level of security for users and applications.

10. References

[1] "IEEE 802.11i." *Wikipedia, The Free Encyclopedia*. 11 Nov 2006, 10:22 UTC. Wikimedia Foundation, Inc. Nov. 25 2006<http://en.wikipedia.org/w/index.php?title=IEEE_802.11i&oldid=87121019>

[2] "Wi-Fi Protected Access 2 Data Encryption and Integrity." Microsoft TechNet. The Cable Guy. July 29 2005. <http://www.microsoft.com/technet/community/columns/cableguy/cg0805.mspx>

[3] "Understanding the updated WPA and WPA2 standards". ZDNet Blogs. Posted by George Ou. June 2 2005. <http://blogs.zdnet.com/Ou/?p=67>

[4] "Deploying Wi-Fi Protected Access (WPA[tm]) and WPA2[tm] in the Enterprise." Wi-Fi Alliance, Feb. 27 2005<http://www.wifi.org/files/uploaded_files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf>

[5] Lehembre, Guillaume. "Wi-Fi security –WEP, WPA and WPA2". Article published in number 1/2006 (14) of hakin9, Jan. 2006. Publication on www.hsc.fr on Dec. 28 2005. <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf>

[6] Ou, George. "Wireless LAN security guide". www.lanarchitect.net. Revision 2.0 Jan 3 2005.<http://www.lanarchitect.net/Articles/Wireless/SecurityRating>

[7] Bulk, Frank. "Learn the basics of WPA2 Wi-Fi security". Network Computing Jan. 27 2006. <http://www.informationweek.com/story/showArticle.jhtml?articleID=177105338>

[8] "Extensible Authentication Protocol." Wikipedia, The Free Encyclopedia. Nov. 26 2006, 15:39 UTC. Wikimedia Foundation, Inc. Nov 27 2006 <http://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&oldid=90231401>.

[9] Gupta, Ashok and Buthmann, Theresa. "The Bell Labs Security Framework: Making the case for End-to-End Wi-Fi Security". Lucent Technologies Sep. 11 2006 (15). <http://www.lucent.com/livelink/09009403800aa8c9_White_paper.pdf>

[10] Epstein, Joe. "802.11w fills wireless security holes". Network World Apr. 3 2006 <http://www.networkworld.com/news/tech/2006/040306-80211w-wireless-security.html>

[11] Wright, Joshua. "How 802.11w will improve wireless security". Network World May 29 2006 <http://www.networkworldcom/columnists/2006/052906-wireless-security.html>

[12] Wright, Joshua. "802.11w security won't block DoS attacks". Tech World Jun. 14 2006 <http://www.techworld.com/security/features/index.cfm?featureID=2599&pagetype=samecatsamchan>

[13] Sood, Kapil and Eszenyi, Mathew. "Secure Management of IEEE 802.11 Wireless LANs". Intel Software Network <http://www3.intel.com/cd/ids/developer/asmo-na/eng/dc/mobile/287462.htm>

[14] Strand, Lars. "802.1X Port-Based Authentication HOWTO". The Linux Documentation Project Oct. 18 2004. <http://tldp.org/HOWTO/html_single/8021X-HOWTO>

[15] Bellardo, John and Savage, Stefan. "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions" USENIX 2003 Nov. 7 2003 <http://www.cse.ucsd.edu/%7Esavage/papers/UsenixSec03.pdf>