WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?

Frank H. Katz
Armstrong Atlantic State University
Department of Information, Computing, and Engineering
11935 Abercorn Street
Savannah, GA 31419
912-344-3192
Frank.Katz@armstrong.edu

ABSTRACT

Significant weaknesses in the Wired Equivalency Protocol (WEP) led to the creation of the Wi-Fi Protected Access (WPA) Wired Local Area Network (WLAN) security protocol and the amendment to that protocol, WPA2. Certified by the WiFi Alliance in 2001, WPA[1] was superseded by WPA2 in 2006[1] as being mandatory for usage with the IEEE 802.11i standard for specifying security for wireless networks. Recent work by Eric Tews of the Technical University of Darmstadt and fellow German security researcher Martin Beck indicate that WPA can be cracked in 15 minutes.[2] Their work tends to confirm that it was necessary to replace WPA with WPA2. However, some features of WPA2 seem to indicate that in some circumstances, WPA2 may be no more secure than WPA. [3]

This paper describes the results of my investigation into the differences between WPA and WPA2, the vulnerabilities and limitations of each, the reasons why WPA2 is considered to be a more robust and secure standard than WPA.

Keywords

Information security, Wireless, Networks, WLAN, WEP, WPA, WPA2, TKIP, AES.

1. INTRODUCTION

The information detailed in the article *Don't Assume WPA2 is more secure than WPA*[3] led me to question whether WPA2 has vulnerabilities, what they are and how they can be mitigated. To that end, this paper will examine how WPA and WPA2 work, illustrating the differences between the two protocols. It will describe how WPA can be "cracked", and if this is possible with WPA2. In doing so, any solutions to this problem will be described, and an analysis of these will be presented in an effort to find the best solution to the problem.

2. HOW WPA AND WPA2 WORK

2.1 WPA

A discussion of how WPA works cannot begin without a brief discussion of why WPA was created to replace the WEP protocol. WPA was created to address several significant problems with WEP.

- WEP uses small key sizes: the key size for WEP encryption is only 40 bits, which is not long enough to resist brute-force attacks.[4]

- **WEP does not include key management:** without key management, keys "tend to be long-lived and of poor quality."[4] The longer a key is used by all nodes on a network, the more likely it is to be cracked.

- **WEP uses the RC4 cipher algorithm:** RC4 is a stream cipher algorithm, which "takes one character and replaces it with another character, the output of which is known as a keystream."[5] In this case, the problem is that the default key being used and a 24-bit Initialization Vector (IV) are combined to create a "seed" for a random number being entered into the RC4 algorithm, and that the 24-bit IV creates 16,777,216 different RC4 cipher streams for one WEP key. This seems like a lot, but that can be "achieved in only a few hours and reuse of the same IV becomes unavoidable."[4]

- It is easy to forge WEP authentication messages: in a strange quirk, turning on authentication when using WEP actually makes it easier to guess the key for system attackers. This situation exists because WEP uses Shared Key authentication, and this "involves demonstrating the knowledge of the shared WEP key by encrypting a challenge." But if the attacker "can observe the challenge and encrypted response, he can "determine the RC4 stream used to encrypt any challenge that would be received in the future."[4]

In order to mitigate and eliminate these security issues, the Wi-Fi Alliance created the Wi-Fi Protected Access (WPA) standard, which has three major improvements over WEP. These improvements are:

- Improved data encryption: this is done through the Temporal Key Integrity Protocol (TKIP), which includes a hashing algorithm that shuffles the keys. It also uses an integrity-checking feature to ensure that the keys have not been altered.[4] Even though "TKIP does use the RC4 stream cipher and all parties must share the same secret key,"[4] this key, called the Temporal Key (TK) must be 128 bits long, much longer than that used in WEP, which is only 40 bits long. Just like WEP, it uses an IV, but this is 48 bits long, double the size that is used in WEP. "Even if the TK is shared, all involved parties generate a different RC4 key stream."[4] TKIP is also known as "per-packet keys," which means that it "dynamically generates a new key for each packet created," which prevents collisions. In fact, TKIP allows for "280 trillion possible keys that can be generated for a given data packet."[5]

- **User authentication:** WPA requires user authentication, while WEP does not. WEP regulates access via a computer's MAC address, which can be easily spoofed or sniffed out and stolen. WPA uses the Extensible Authentication Protocol (EAP), which uses public key encryption, to authenticate users to the network. As specified in RFC 3748, EAP[6] runs directly over data link layers and involves the sending and receiving of requests and responses between peers in a network to perform the authentication. EAP handles the authentication by using unique usernames/passwords, digital certificates, and smart cards or "whatever credential the IT administrator is comfortable in deploying."[7]

- **Integrity:** ensured by the Message Integrity Code (MIC) for TKIP. This is computed by a new algorithm named "MICHAEL". The MIC is computed to "detect errors in data contents, either due to transfer errors or due to purposeful alterations."[4]

2.2 WPA2

In September 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2). This was based on the final IEEE 802.11i standard ratified in June 2004. There are some similarities between WPA and WPA2. Like WPA, WPA2 uses 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.[7]

One difference between WPA and WPA2 is that WPA2 uses a mixed mode that supports both WPA and WPA2 enabled devices on the same wireless network.

However, the most significant difference between WPA and WPA2 is WPA2's use of the Advanced Encryption Standard (AES) instead of TKIP for data encryption. AES, as described in the 802.11i standard, is a block cipher, as opposed to RC4, used in WEP and WPA, which is a stream cipher. While a stream cipher only executes against one character at a time, a block cipher operates against an entire block of text all at once. A "substitution permutation network," AES has a fixed block size of 128 bits[8] and three different key sizes, each used in the three different "rounds" or iterations of the algorithm. In the first iteration a 128-bit key is used to perform 9 rounds, in the second a 192-bit key performs 11 rounds, and in the third iteration a 256-bit key is used to perform 13 rounds. Because AES is a substitution cipher, "within each round bits are substituted and rearranged and then special multiplication is performed based on the new arrangement."[5] The effectiveness of AES cannot be disputed – the time needed to break it by using a brute force attack with $1 million worth of microprocessors and a 128-bit key length is 2.20 x 10^{17} years. With a 192-bit key length, the time increases to 10^{36} years.[5]

3. CRACKING WPA

In March 2009, security researchers Eric Tews and Martin Beck published an article, *Practical Attacks Against WEP and WPA* at WiSec '09, the second ACM conference on Wireless network security. In this article they detailed how they were successfully able to crack WEP and WPA, which heretofore had been deemed to be unbreakable. Of utmost significance was that their attack on WPA did not involve the use of a dictionary attack, which is defined as "an attempt at password guessing where the attackers take each word from a dictionary and encodes them the same way that the passphrase was encoded. When attackers find a match, they know which dictionary word made up the passphrase."[5]

Rather, this attack has been considered the first cryptographic attack on WPA and specifically, TKIP. Their attack was reported initially in various online media including Network World. Network World reported that rather than attempt a dictionary attack, Tews and Beck were able to crack the TKIP key. "According to Dragos Fuiu, the PacSec organizer, in order to crack the TKIP key, the researchers found a way to trick the router into sending them large amounts of encrypted data. Combining this with what Ruiu calls a "mathematical breakthrough", the attack time was reduced to a matter of minutes, between 12 and 15."[9]

In their paper, Tews and Beck postulated that it was possible to "decrypt traffic in a chopchop like manner and to send packets with a custom content."[10] A chopchop attack is one in which a WEP data packet is decrypted without knowing the key. It does not recover the key itself, but just reveals the plaintext.

Tews and Beck described how this could be done: "an attacker would first capture network traffic until he has found an encrypted Address Resolution Protocol (ARP) request. These packets can be easily detected because of their characteristic length. The source and destination Ethernet addresses are not protected by WEP and TKIP and ARP requests are always sent to the broadcast address of the network. Most of the plaintext of this packet is known to the attacker, except the last byte of the source and destination IP addresses, the 8 byte MICHAEL MIC and the 4 byte ICV checksum. An attacker can now launch a modified chopchop attack as against a WEP network to decrypt the unknown plaintext bytes." [10]

They further state that after a chopchop attack is executed, a guess is made as to the contents of the last byte of the packet. "If the guess was correct, a MIC failure report frame is sent to the client, but the TSC counter is not increased. The attacker needs to wait for at least 60 seconds after triggering the MIC failure report frame to prevent the client from engaging countermeasures. Within a little bit more than 12 minutes, the attacker can decrypt the last 12 bytes of plaintext (MIC and ICV)."[10] After this has been done, all the attacker has to do is "simply reverse the MICHAEL algorithm and recover the MIC key used to protect packets being sent from the access point to the client."[10]

A simpler description of Tews' and Beck's work is that TKIP is dependent upon calculating checksums in order to ensure the integrity and accuracy of transmitted data. In their method, "an attacker sniffs a packet, makes modifications to affect the checksum, and checks the results by sending the packet back to the access point." [11] Checksums take a sequence of numbers, apply a conversion to produce a short result, and append that result to the transmission. As an example, if you were transmitting a book's 13 digit ISBN beginning with 978, "twelve of the digits represent a unique book number. The 13th digit is a base 10 number derived from alternately multiplying successive digits by 1 or 3, adding the results, and taking the modulo of 10. If the ISBN is typed incorrectly, a system that recalculates the checksum can determine if digits are swapped or wrong digits are entered."[11] So just like hash values are used to confirm digital certificates, checksums are used to confirm the integrity of the packet being transmitted. "If the payload changes and the checksum does not, the packet has been tampered with."[11]

As described above, TKIP uses the MICHAEL algorithm (MIC) as a second layer to verify the integrity of the packet. To prevent chopchop, it forces a client to respond after it receives two consecutive bad MICHAEL checksums within 60 seconds. If it does, the client will shut down for 60 seconds and then request a new key exchange with the Access Point (AP). An AP faced with the same situation will also shut down for 60 seconds and then rekey every client. Tews and Beck were able to circumvent the system because WEP and TKIP are used one after the other and because Michael code is contained in the packet that's being checksummed by WEP, an attempt to crack the packet can first use chopchop without setting off the MICHAEL countermeasures.[11]

4. CAN WPA2 BE CRACKED LIKE WPA?

Tews and Beck have proven that WPA, and more specifically, its TKIP encryption method can be cracked. The primary difference between WPA and the more robust WPA2 standard is the method of packet encryption. WPA2 uses the AES encryption method. As described previously, AES is a block cipher that uses successively longer key bit sequences to encrypt packets as they are being transmitted. The advantage of WPA2 over WPA is that WPA2 does not include the TKIP encryption algorithm, which includes the RC4 bit-by-bit stream cipher methodology. The AES block cipher iterative encryption algorithm as implemented in WPA2 is considered to be so strong an encryption standard that the National Security Agency uses its 192-bit and 256-bit key lengths to encrypt Top Secret documents.[12] For now and into the foreseeable future, the use of AES as implemented in WPA2 should be considered to be unbreakable.

There has been one obstacle to the implementation of WPA2 that needs to be overcome by organizations seeking to improve their WLAN's security. This has more to do with the implementation of WPA than the technical details of how it encrypts data. This is that the Wi-Fi Alliance never intended for WPA to be anything more than an intermediate standard. It is a subset of the 802.11i standard and was created to reduce the costs of adoption because WPA could accommodate older WEP hardware. Implementation of the more secure WPA2 standard requires newer hardware. Indeed, before the implementation of WPA2, the Wi-Fi Working Group (WG) defined WPA, "which is a WEP wrapper design, to fix all the known problems with WEP. It has been established that WPA cannot fulfill the original WEP design goals, because the available CPUs on existing hardware are too limited."[13] Given that TKIP was introduced in 2003, and the Wi-Fi WG introduced WPA2 with its AES encryption in 2004, enterprise users have had five years to upgrade their hardware to accommodate the WPA2 requirements. Current CPUs will support WPA2, and enterprise users and organizations should implement WPA2 on their WLANs as soon as possible.

5. CONCLUSION

As previously described, the WPA encryption protocol can be cracked due to vulnerabilities in the TKIP encryption algorithm. After analyzing the WPA and WPA2 wireless encryption protocols and enumerating their differences, it is clear that the Advanced Encryption Standard, which is an integral component of the WPA2 protocol, is a significant improvement over WPA's TKIP. Current technology is adequate to ensure that organizations can implement WPA2, and organizations that use WPA should consider implementing WPA2.

6. REFERENCES

[1] Figueroa, Edgar, *Wi-Fi Certified Makes it Wi-Fi: An Overview of the Wi-Fi Alliance Approach to Certification,* Wi-Fi Alliance®', September 2006

[2] Moscaritolo, Angela, *Vulnerability discovered in WPA encryption,* retrieved July 29, 2009 from http://www.securecomputing.net.au/News/127719,vulnerability-discovered-in-wpa-encryption.aspx

[3] Naraine, Ryan and Danchev, Dancho, *Don't assume WPA2 is more secure than WPA,* retrieved July 27, 2009 from http://blogs.zdnet.com/secuirty/?p=826&tag=rbxccnbzd1

[4] Bulbul, H, Batmaz, I., and Ozel, M., Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (robust Security Network) Security Protocols, In *Proceedings of the 1st international conference on Forensic applications and techniques, information, and multimedia and workshop,* (Adelaide, Australia, January 21-23, 2008), ICST, Brussels, Belgium, 2008, p. 1-6

[5] Ciampa, Mark, CWSP Guide to Wireless Security, Course Technology, Boston, MA, 2007, p. 45, 53, 149, 151

[6] RFC Archive, retrieved August 2, 2009, from http://www.rfc-archive.org/getrfc.php?rfc=3748

[7] *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks,* Wi-Fi Alliance®', April 29, 2003, 5-7

[8] OPENXTRA, *WPA vs WPA2 (802.11i): How your Choice Affects your Wireless Network Security,* retrieved August 2, 2009 from http://www.openxtra.co.uk/articles/wpa-vs-80211i

[9] KezNews forum, *WPA Encryption No Longer Secure,* retrieved August 2, 2009, from http://keznews.com/5041_WPA_Encryption_No_Longer_Secure

[10] Beck, M and Tews, E, Practical Attacks Against WEP and WPA, In *WiSec'09: Proceedings of the second ACM conference on Wireless network security,* (Zurich, Switzerland, March 16-19, 2009), ACM, New York, NY, p. 83-84

[11] Fleishman, Glenn, *Battered, but not broken: understanding the WPA crack,* retrieved August 2, 2009, from http://arstechnica.com/security/news/2008/11/wpa-cracked.ars

[12] *FACT SHEET, CNSS Policy No. 15, Fact Sheet No. 1 National Policy on the Use of the Advanced Encryption Standard to Protect National Security Systems and National Security Information,* June 2003, p. 2

[13] Moen, V, Raddum, H, and Kjell, J, Weaknesses in the temporal key hash of WPA, In *ACM SIGMOBILE Mobile Computing and Communications Review, Volume 8, Issue 2* (April 2004), ACM, New York, NY, p. 76