WPA 3 - Improvements over WPA 2 or broken again?

Maximilian Appel, Dr.-Ing. Stephan Guenther*
*Chair of Network Architectures and Services, Department of Informatics
Technical University of Munich, Germany
Email: m.appel@tum.de, guenther@tum.de

***Abstract*—Due to the widespread usage of WiFi, securing them is and will continue to be an important task. After it was signed into IEEE 802.11 in 2004, WPA2 became the commonly used encryption standard for WiFi networks, replacing the originally as temporary solution conceived WPA. It's successor WPA3 was released in June 2018. At the time of writing it has not found widespread adoption yet. This paper aims to provide an overview on the designs of WPA2 and WPA3, including their currently known vulnerabilities. And tries to come to a conclusion on whether WPA3 is still a viable successor or if it has already been compromised beyond repair.**

***Index Terms*—wireless networks, WPA2, WPA3, Encryption, KRACK-Attack, Dragonblood-Attack**

1. Introduction

Created as a guideline for wireless connected networks in 1997, IEEE 802.11 also defined security protocols for such networks and as such has been revised multiple times in reaction to emerging technologies and attack methods. The original security mechanism WEP was replaced in 2003 in favor of the at them time new WPA. The main reason for this was the discovery of major weaknesses in the RC4 encryption algorithm, that WEP was based on. However, this was only an intermediate measure meant to strengthen security during the creation process for a full amendment to the the standard. The full standard was signed in 2004 as IEEE 802.11i, also more commonly known as WPA2. This amendment officially deprecated WEP and even forbids the implementation in new devices. However because of the higher hardware requirements of its successors it partially remains in use to this day. In 2018 WPA3 was announced as the replacement for WPA2, meant to solve known problems and vulnerabilities. The full protocol was released in June 2018 and is, at the time of writing, the currently recommended security standard for wireless networks. The rest of this paper first provides a detailed description of WPA2 and WPA3. This is followed by a brief analysis of the currently known vulnerability for each of them. It is then concluded with a discussion on whether or not WPA3 is still a viable security scheme. [1]

2. WPA2

Signed as IEEE 802.11i in 2004, WPA2 marked a large step forward not only in terms of security, but also in terms of hardware demands. The main reason for the latter is the utilization of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which uses the Advanced Encryption Standard (AES) block cipher for its data encryption. Both of which are described in more detail in the following sections. Temporal Key Integrity Protocol (TKIP) is still available under WPA2, in order to provide backward compatibility to WPA capable devices that possess insufficient processing power for AES.

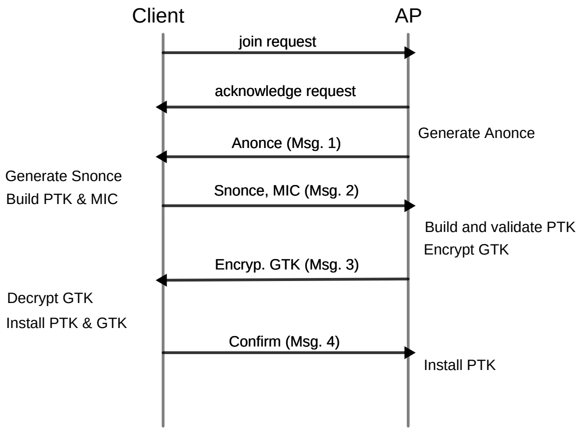

Figure 1: diagram showing the steps of the four-way handshake

2.1. Authentication

WPA2 handles authentication via two separate types of keys, which are used for the decryption and encryption of messages. Pairwise Transient Keys (PTKs) that are used for unicast messages and as such are only known to the AP and a single client. The other type is the Groupwise Transient Key (GTK), a single key that is used for multicasts and broadcast, and therefore is known by the AP and all clients in the network. In order to generate and distribute these keys WPA2 uses two separate handshake protocols. The so called four-way handshake is executed first and generates and distributes the PTK. A simple handshake that is secured with the individual clients PTK, is used to update and distribute the GTK from the AP to the clients. The four-way handshake (see figure 1) begins under the assumption that both the client and the AP possess a shared Pairwise Master Key (PMK), which consists of a PBKDF2 function value of the network's

doi: 10.2313/NET-2020-11-1_02

passphrase, the networks Service Set Identifier (SSID), and the Hash Message Authentication Protocol (HMAC) function used to stretch the passphrase. First the client sends a connection request to the AP, which is then answered with an acknowledgment. Afterwards the client generates a nonce (Anonce), a randomly generated value that prevents message replay attacks, and sends it to client. The client then generates a nonce of its own (Snonce) and uses it to generate the PTK, by concatenating both nonces, the PMK and the mac addresses of both AP and client. In the next step the client uses the PTK to generate a Message Integrity Code (MIC) and then sends the Snonce along it to the AP. The AP then uses the received Snonce to generate the PTK, in the same way the client did. After that it uses the PTK and the Snonce to derive a MIC, which is then compared to the MIC that was received with the Snonce. If either of the nonces was manipulated by an attacker, the MICs will not match and the handshake is aborted. Due to the random nonces role in the generation Process, the generated PTK will always be unique for the individual session. At the end of the four-way handshake, the AP uses the freshly established PTK to safely transmit the current GTK. This completes the client's authentication. [2]

2.2. AES

The Advanced Encryption Standard (AES) defines a secure block cipher encryption algorithm. AES was chosen in 2001 at the end of the AES selection process as the standard for safe encryption by the US government. AES supports various key sizes (128bit, 192bit, and 256bit) and handles data in blocks. The block's sizes are independent of the chosen key size. A complex algorithm is used to enlarge the initial key into several 128bit large keys. All but one of these keys are then used in separate encryption rounds, each of which consists of three substitutions and one permutation. The total number of rounds depends on the used key size (see table 1). The remaining unused key is later used to start the decryption process. [1], [3]

2.3. CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an implementation of the standards of the IEEE 802.11i amendment. It protects the confidentiality of the data by using AES in counter mode and uses CBC-MACs to assure authenticity and integrity of the messages. It therefore provides protection for confidentiality, authenticity and integrity. The protocol first takes a key, which in WPA2's case is either a PTK or the GTK, and additional data necessary for the protocol and runs them through AES in counter mode. Counter mode refers to a specific algorithm that turns a block cipher into a stream cipher. The in this way generated keystream is then combined with the plaintext in an XOR operation to build the encrypted ciphertext. (see figure 2) [1]

2.4. Vulnerabilities

This section provides a brief overview on WPA2s known weaknesses. For the sake of brevity, we are limiting this section to attacks that allow attacks on APs without prior knowledge of the password.We are also excluding the KRACK-Exploit, because patches that secure APs against it are available under WPA2.

TABLE 1: Number of encryption rounds for AES key sizes

AES key size	Number of rounds
128 bit	10
192 bit	12
256 bit	14

2.4.1. Deauthentication Attack.

Session management frames are system messages between clients and APs used for communication. Once type of management frame are de-authentication frames which are normally sent by client and AP to signal the end of a session. Under WPA2 session management frames are sent encrypted without authentication. By spoofing the clients and the AP's MAC address and then sending false Deauthentication frames, an attacker can cause both AP and client to cease communication with each other. [1]

2.4.2. Handshake Capture Dictionary Attack.

The four-way handshake generates the PTK by combining two randomly generated nonces with the otherwise completely static PMK. Because the nonces are sent in plaintext, an attacker can gain enough information to perform off-line dictionary and brute-force attacks against the passphrase by eavesdropping on an successful handshake. In theory this still requires an attacker to wait for a handshake that he can capture. However, by using the previously mentioned Deauthentication Attack to disconnect an already authenticated client the attacker is able force a the client to perform a four-way handshake, which he then can capture. [1]

2.4.3. PMKID Hash Dictionary Attack.

During the authentication phase of WPA2, but before the actual four-way handshake, the AP sends the client a Extensible Authentication Protocol over LAN (EAPOL) frame. This frame contains the titular Pairwise Master Key Identification (PMKID). The PKMID is a hash value derived from the PMK, a static String, the clients MAC address and the AP's MAC address. An attacker can use the PKMID to perform dictionary and brute-force attacks against the networks passphrase by simply calculating the hash with a candidate passphrase and comparing the result with the PKMID. [1]

3. WPA3

Published in 2018, WPA3 is mostly build upon its predecessor and as such only makes minor changes to the decryption standards. For the sake of brevity this paper only focuses on the big changes in the authentication protocol. This is then followed by a description of the relatively recently discovered vulnerabilities: the Dragonblood-Attacks.

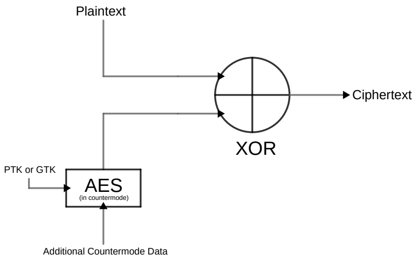

Figure 2: diagram showing the encryption process with CCMP

3.1. Authentication

WPA3 changes the authentication protocol by adding an additional layer of security in form of the Simultaneous Authentication of Equals (SAE) handshake, a variant of the Dragonfly Handshake. The Dragonfly Handshake was originally developed by Dan Harkins in 2008 as Password Authenticated Key Exchange (PAKE) for mesh networks and as such turns a shared plaintext password into a secure cryptographic key. Dragonfly supports Elliptic Curve Cryptography (ECC) and Finite Field Cryptography (FFC). Because ECC is the more common option and the general similarities between the two, this paper only contains a description of ECC.

3.1.1. Elliptic Curve Cryptography.

Dragonfly uses elliptic curves over a prime field (ECP groups) in its ECC mode. ECP groups are defined over a prime p and the parameters a and b for the polynomial

$$y^2 = (x^3 + ax + b) \bmod p$$

The key is generated out of the shared password by calculating a combined hash over the pre shared password, an increment counter and identities (IDs) of the client and the AP. In WPA3 the identities are the client's MAC address and AP's MAC address. That hash is then used as the x value in an attempt to find a corresponding y value. If that attempt is unsuccessful, the hash is recalculated with an increased counter. After this another attempt with the new x value is made. This strategy is repeated until a y value is found. The calculated point (x,y) is then used as the password (P) in the Dragonfly Handshake. [4]

3.1.2. The Dragonfly Handshake.

The handshake consists of two phases. The commit phase occurs first and can be initiated by both parties, although in WPA3-personal the client will always send the first commit, while in enterprise mode the radius server commits first. For the commits each of the peers chooses two random values within the interval [2,p] , a private r_i and a mask m_i such that $s_i = r_i + m_i \epsilon$ [2,p]. They then calculate the value $E_i = -m_i \cdot P$ and send it along with their respective s_i to each other. After having received the commit frames, both participants validate the received values and abort the entire handshake in the case of an incorrect value. In the confirm phase the parties use the exchanged data to calculate the secret point K with the formula $K = r_i(s_j P + E_j)$ ($_j$ denoting the parties own value and $_j$ denoting the received values) and hashes its x coordinate to get the key k. They then calculate a HMAC c_i over all the data that has been generated and exchanged during the handshake, utilizing k as key. The parties then exchange and check their corresponding c_i's in a confirm frame, which is discarded in the case of an unexpected value. If the values are correct, the handshake has succeeded and k is the resulting key (see figure 3. [4]

The key k is then used as PMK in WPA2s four way handshake, which is now more secure than before due to the much higher entropy of the PMK. This also enables backward compatibility with devices that are unable to perform the calculations necessary for the Dragonfly Handshake, by setting the AP into a Transition-Mode to merely advertise the Dragonfly Handshake as part of optional Management Frame Protection (MFP) to the clients, although actually all WPA3 capable devices are forced to use the MFP, despite it being advertised as optional. [1]

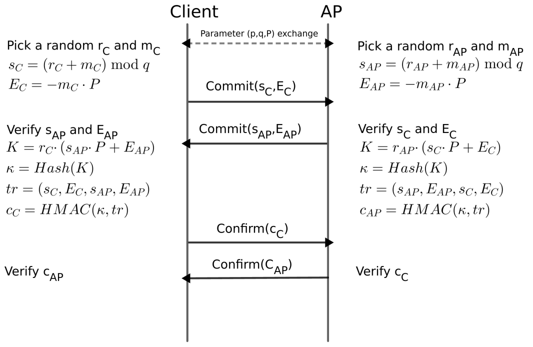
Client
AP
Parameter (p,q,P) exchange
Pick a random r_C and m_C
$s_C = (r_C + m_C) \bmod q$
$E_C = -m_C \cdot P$
Pick a random r_{AP} and m_{AP}
$s_{AP} = (r_{AP} + m_{AP}) \bmod q$
$E_{AP} = -m_{AP} \cdot P$
Commit(s_C,E_C)
Commit(s_{AP},E_{AP})
Verify s_{AP} and E_{AP}
$K = r_C \cdot (s_{AP} \cdot P + E_{AP})$
$\kappa = Hash(K)$
$tr = (s_C, E_C, s_{AP}, E_{AP})$
$c_C = HMAC(\kappa, tr)$
Verify s_C and E_C
$K = r_{AP} \cdot (s_C \cdot P + E_C)$
$\kappa = Hash(K)$
$tr = (s_{AP}, E_{AP}, s_C, E_C)$
$c_{AP} = HMAC(\kappa, tr)$
Confirm(c_C)
Confirm(C_{AP})
Verify c_{AP}
Verify c_C

Figure 3: a diagram detailing the WPA3 SAE Handshake between a connecting client and an AP. In theory either parties can initiated the handshake, but we assume the standard case of the Client sending the first commit. The Calculations shown assume that an ECP group is used.

3.2. Dragonblood

The Dragonblood attacks refer to a number of weaknesses in the WPA3 security scheme's personal mode. They were published by Mathy Vanhoef and Eyal Ronen in April 2019. Dragonblood consists of several different types of attacks.

3.2.1. Downgrade Attacks.

Downgrade attacks target WPA3 networks that are set into the earlier mentioned transition mode. Normally this mode allows devices that are incompatible with the SAE protocol to still connect to the AP under WPA2, while forcing all devices that are able to, to use WPA3. However, by setting up an impostor network with the same ID that only supports WPA2, even WPA3 capable clients are tricked into using WPA2. By catching parts of the WPA2 handshake they are able to once again perform dictionary and brute force attacks against the passwords of WPA3 networks. [4]

3.2.2. Security Group Downgrade Attack.

During the commit phase of the Dragonfly Handshake, the initiator, which in case of WPA3 is usually the client, sends his first commit frame with his preferred security group. If the AP doesn't support this specific security group he answers with a decline message, forcing the client to use a different possibly unsafer group instead. This is done until the AP accepts the offered group. By catching the clients commits and sending fake denial messages, an attacker is able to force the client into using a group of his choice. [4]

3.2.3. Cache-Based Side-Channel Attack.

These attack require an attacker to be able to observe the memory access pattern of one of the parties of the Dragonfly Handshake. The memory access patterns during the generation of a commit frame allow an attacker to gain information about the used password. This information can be used for dictionary attacks that compare the observed patterns with the expected patterns of a to be guessed password. [4]

3.2.4. Timing-Based Side-Channel Attack.

When using certain security groups, the time it takes for an AP to response to a commit frame depends on the used password. This leaked information allows an attacker to perform a variant dictionary attack, by comparing the expected time for a password with the AP's actual response time. [4]

3.2.5. Denial-of-Service Attack.

Due to the high computational cost in the Dragonfly Handshakes commit phase, an attacker can very easily overload an AP by sending bogus commit frames. This leads to high CPU usage on the AP, which in turn can cause delays or even prevention in the regular use of the AP. These attacks can be worsened, depending on if and how defenses against the previously described side channel attacks are implemented, due to the necessity of additional computations. [4]

3.2.6. Possible Fixes.

The downgrade attack against the transition mode, while in theory only temporary, is still highly problematic. Because it is to be expected that the adoption of WPA3 to the point of the full on deprecation of WPA2 will at least take several years. Until that point however most WPA3 networks will likely be used in transition mode. Meaning that unless this vulnerability is closed, all of these APs will be vulnerable to dictionary and brute-force attacks. As already mentioned and shown by the followup research made after the original publication, implementing WPA3 with defenses against the currently known side channel attacks without introducing new ones has proven rather difficult and tedious. They also have shown to increase WPA3's already high computational requirements even further, which poses problem for devices that are unable to implement them. [4]

4. Conclusion

WPA3 was meant to solve most of the vulnerabilities that WPA2 had. None of the known WPA2 specific attack methods went unaddressed and all of the vulnerabilities described in the WPA2 section 2.4 were fixed. Due to the additional security provided by the Dragonfly Handshake, it was considered to be almost impossible to crack the password of a WPA3 network. However Dragonblood revealed major flaws within the WPA3 security scheme that in our opinion cast serious doubt on its long term viability as a security standard. At the time of writing WPA3 is prone to implementation errors, which make side-channel attacks possible. In addition to that WPA3 also has two known conceptional faults, that make the side channel leaks even worse. Although technically temporary the downgrade attack against the transition mode remains especially worrisome, since transition mode can be expected to be the most common use case for at least the next several years. In total all of these vulnerabilities make dictionary and brute-force attacks on the passphrase once again possible, negating one of the biggest advantages WPA3 had over WPA2. All of this has lead us to believe that WPA3 in its current form should not be a long term solution and either has to amended in order to fix the currently known problems or possibly even abandoned in favor of an alternative improved scheme. Implementing additional defenses under WPA3 have proven to be problematic and even partially impossible on already existing WPA3 hardware. Meaning that expensive hardware upgrades might become necessary. All of this makes WPA3's future seem highly uncertain, as it will depend on the feasibility of possible solutions, which warrants further research. Despite these issues with WPA3 our conclusion is still that WPA3 is a considerable improvement over WPA2 in terms of security and should remain in service for the time being.

References

[1] T. H. Christopher P. Kohlios, "A Comprehensive Attack Flow Model and SecurityAnalysis for Wi-Fi and WPA3," *Electronics*, vol. 7, no. 11, 2018.

[2] M. Gast, *802.11 Wireless networks: the definitive guide, 2nd edn.* O´Reilly Media, Inc., 2005.

[3] "FIPs PUB 179: Announcing the ADVANCED ENCRYPTION STANDARD (AES)," November 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[4] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd," in *IEEE Symposium on Security & Privacy (SP)*. IEEE, 2020.