Research Seminar in Cryptography

Report on 'Security of WiFi networks'

Mattias Lass

Supervisor: Danielle Morgan

November 29 2019

1 Introduction

Modern Wi-Fi networks generally use WPA2 to protect transmitted data. However, because WPA2 is more than 14 years old, the Wi-Fi Alliance recently announced the new and more secure WPA3 protocol. WPA3 promises to solve some of the issues with WPA2 but several problems have already been found with WPA3. This report aims to give an overview of some of these weaknesses, specifically the weaknesses discovered by Vanhoef and Ronen in 2019 [1]. In addition this report provides a brief introduction to WPA2 and WPA3 which should be understandable to a reader unfamiliar with the topic.

The remainder of this report is organized as follows:

- Second section gives a high-level overview of WPA2, mainly focusing on the key establishment algorithms of WPA2;
- In the third section WPA3 is covered in a similar way;
- Sections four and five describe weaknesses in WPA2 that WPA3 aims to solve;
- Sections six through eight cover WPA3's weaknesses discovered in 2019 by Vanhoef and Ronen [1]. It should be noted that the report at hand is mostly based on the Vanhoef's and Ronen's paper and does not contain any original work;
- In the last section a conclusion made whether WPA3 improves on WPA2.

2 WPA2

After it was shown that the Wired Equivalent Privacy (WEP) is broken, the IEEE offered a more robust solution in the 802.11i amendment to the Wi-Fi standard. Based on this standard the WPA certification was created. It's final version was released in 2004 and is called WPA2. [2]

The WPA2 amendment establishes a key exchange protocol called the 4-way handshake and defines some data-confidentiality protocols which are used to encrypt traffic between an wireless access point and a client.

2.1 Pairwise Master Key

In a WPA2 connection the mutual authentication between the supplicant (the client) and the authenticator (the access point) is based on a shared secret called the Pairwise Master Key (PMK). In an enterprise network the PMK is negotiated using an authentication server. In a personal network the PMK is derived from a pre-shared password. [2]

The password can either be a 32 digit hexadecimal number (64 bytes) or a 8 to 63 byte long passphrase. The 32 digit number is used directly as the PMK. The passphrase is used to derive the PMK using the Password-Based Key Derivation Function 2 (PBKDF2) as follows:

$$PMK = PBKDF2(passphrase, ssid, ssidLength, 4096, 256)$$

This means that the passphrase, SSID of the network and the length of the SSID(the identifier of the network) are concatenated and hashed 4096 times to produce a value of 256 bits.[3]

2.2 4-way handshake

The PMK, covered in the previous section, is used in what is called a 4-way handshake to derive a Pairwise Transient Key (PTK). The PTK is used to encrypt and decrypt unicast messages between the client and the access point. As the name implies, four messages are sent in the 4-way handshake, this process is illustrated by figure 1. [2]

The authenticator initiates the 4-way handshake with the first message. This message contains only an authenticator nonce (ANonce), which is a random number generated by the authenticator. This message is completely unsecured. [2]

The supplicant then generates the supplicant nonce (SNonce) and sends it as the second message. As the PTK is derived from PMK, ANonce, SNonce and the MAC addresses of the authenticator and the supplicant, the supplicant can calculate the PTK before sending the second message. This allows the supplicant to add a Message Integrity Code (MIC) to the second message. Both of the following messages will also contain an MIC. [2]

After having received the second message the authenticator can also calculate the PTK. The authenticator sends the third message which contains a Group Temporal Key, which is used for multicast traffic [2]. This key will not be further covered in this report however, the third message plays a crucial part in one of the main vulnerabilities of WPA2.

Finally the supplicant replies with the fourth message, which is a simple acknowledgement that the third message was received. The supplicant installs the PTK after it sends out the fourth message. The authenticator installs the PTK after having received the fourth message. [2]

2.3 Data-Confidentiality Protocols

WPA2 can use three different data-confidentiality protocols to guarantee the confidentiality and integrity of the messages or in other words to encrypt traffic between the access point and a client. The first protocol is Temporal Key Integrity Protocol (TKIP), however this has been deprecated due to security concerns from 2015 and will not be covered further in this report. [2]

The second protocol is called CCMP. This is based on the AES-CCM mode. It is an Authenticated Encryption with Associated Data (AEAD) algorithm which is secure as long as no Initialization Vector (IV) is repeated under a particular key. In CCMP a 48-bit nonce and some additional parameters are used as the IV. The nonce is also used as a replay counter by the receiver, incremented by one before sending each message. It is initialized to 0 when installing the PTK. [2]

The third protocol is GCMP which is based on AES-GCM. It is also an AEAD algorithm and as the IV a 48-bit nonce with additional parameters is used. The nonce is created in the same way as in CCMP. Note that this is also only secure as long as no IV is repeated under a particular key. [2]

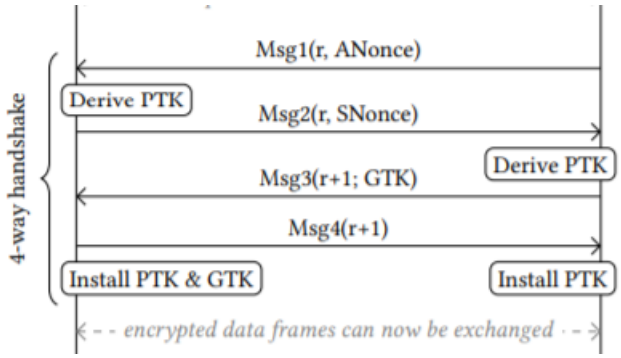

Figure 1: The 4-way handshake. Here the supplicant is on the left and the authenticator is on the right. [2]

3 WPA3

WPA3 was released as a successor of WPA2 after in 2018. It does not define any new protocols. Instead it removes the deprecated TKIP. It also mandates support for the Dragonfly handshake, which was defined in an earlier standard and replaces the pairwise master key derivation from WPA2-personal. Another mode mandated by WPA3 is a transition mode in which WPA2 and WPA3 are simultaneously supported. In other aspects WPA3 is the same as WPA2. [1]

3.1 Dragonfly handshake

In WPA3 the PMK used for the 4-way handshake is derived using the Dragonfly handshake. The variant of the handshake used in WPA3 is also known as Simultaneous Authentication of Equals (SAE). Unlike the PMK derivation process in WPA2 the SAE provides forward secrecy. This means that simply knowing the network passphrase and sniffing the network messages is not sufficient to decrypt any of the messages. [1]

The Dragonfly handshake turns a password into a high-entropy key. Dragonfly supports both Elliptic Curve Cryptography and Finite Field Cryptography with multiplicative groups modulo a prime (MODP). Before the handshake is initiated the pre-shared password is converted to a group element using a hash-to-element method. This method has an internal loop which could run a different number of iterations depending on the passphrase. To avoid

leaking information about the passphrase via the length of time it takes to run this method, the number of iterations of the loop is set to a constant. In practice this means making the loop run extra iterations if the method finishes early. [1]

The Dragonfly handshake itself consists of a commit and confirm phase. In the commit phase both the AP and the client pick two random numbers which are used to add sufficient entropy to the passphrase. Both parties perform a commit message based on these numbers. In the confirm phase the actual key is calculated. The parties then calculate an HMAC over the summary of the handshake and send it to the other side verifying that the same key was agreed upon. This process is illustrated by figure 2 where P denotes the result of the hash-to-element method. [1]

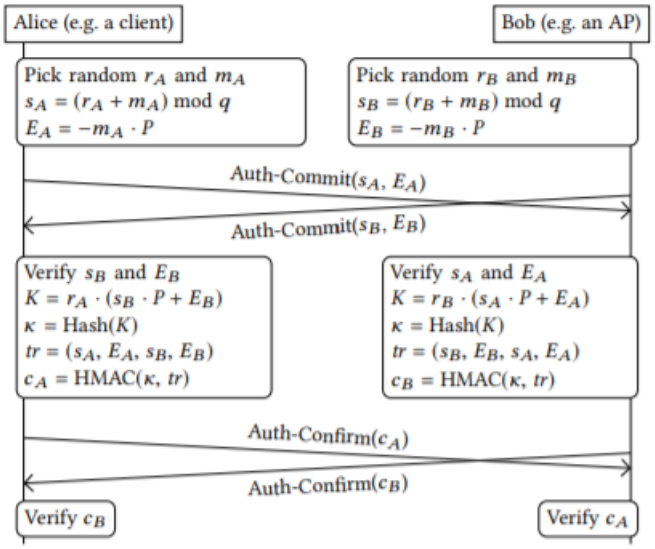

Figure 2: Simultaneous Authentication of Equals. Note that the handshake is symmetrical and no actual information about the original passphrase is sent to the other party. [1]

4 Key Reinstallation Attacks

In 2017 the KRACK Key Reinstallation Attack (KRACK) was disclosed by Vanhoef and Piessens [2]. This attack relies on a design flaw in the 4-way handshake. By forcing the authenticator to resend the third message of the handshake it is possible to make the supplicant resend the fourth message. This re-installs the same PTK. This is a problem since the install also sets the nonce counter to 0, which means that a nonce will be re-used under the same key. This violates the security assumptions of both the CCMP and GCMP protocols allowing for some messages to be decrypted.

It seems to be a common misconception that the Dragonfly handshake replaces the 4-way handshake and thus WPA3 eliminates this vulnerability. This however is not true since in WPA3 Dragonfly handshake is only used to derive the PMK. The 4-way handshake is still

used in WPA3 to derive the PTK.

Instead WPA3 routers can be set up to not allow the re-transmission of the third message of the handshake [4]. This negates the attack in the expense of the usability of the protocol. Thus it seems it is still possible to set up a WPA3 network which is vulnerable to the KRACK.

Moreover the same mitigation has been deployed on WPA2 APs [4]. Therefore it cannot actually be said that WPA3 is meant to address this vulnerability.

5 Lack of Forward Secrecy and Dictionary Attacks

A common setup for the WPA2 personal networks is to use a passphrase as a pre-shared secret. This is used as a parameter to derive the PTK which is used to secure all messages in a connection between a client and an access point. In fact this is the only such parameter that is a secret - the rest can easily be obtained via packet sniffing. This leads to two problems. Firstly anyone who is in the possession of the passphrase can read and forge any messages in the network - there is no forward secrecy. Secondly using a weak passphrase leaves the network vulnerable to an offline dictionary attack. [3]

The attacker only needs to sniff any message, except for the first, of the the 4-way handshake to perform a offline dictionary attack. They are then in possession of an MIC and all of the parameters it was calculated from, except for the passphrase. They can start checking all possible passphrases to see if any produce the same MIC. [3]

WPA3 aims to solve both problems. The Dragonfly handshake produces an undeterministic key. Therefore all keys used in WPA3 connections are different thus not allowing an authenticated party full control over the network - WPA3 provides forward secrecy. Since secret random parameters are used to derive the key in the Dragonfly handshake, it also prevents offline dictionary attacks. [1]

However, WPA3 also defines a transition mode which accepts both WPA3 and WPA2 connections with the same password. It is possible to trick a client into thinking that an AP only accepts WPA2 connections by creating a rogue AP that pretends to be part of the network. The rogue AP then broadcasts that the network is a WPA2-only network. If a client connects to this network the 4-way handshake is initiated and the second message will be sent to the rogue AP. Therefore the transition mode of the WPA3 does not actually provide a guard against offline dictionary attacks against the passphrase. [1]

The Wi-Fi Alliance has accepted that this attack is possible and the official recommendation is to not use the WPA3 transition mode [5]. Instead if WPA2 and WPA3 are to be used concurrently, two different networks with different passwords should be used. If WPA3 becomes widely adopted the necessity to use the transition mode decreases, thus this downgrade attack should become more irrelevant as time passes.

6 Group Downgrade Attack

The SAE handshake can be performed using different elliptic curve or multiplicative groups. The 802.11 standard allows APs to prioritize groups in a user-configurable order. Unfortunately the group negotiation process is never cryptographically validated allowing for an man-on-the-side attack. [1]

The attacker can block client group negotiation messages from arriving to an AP. Then the attacker can respond with a forged response claiming that the AP does not support the requested group. This allows for the attacker to have some control over which group is selected. Usually the attacker might force the use of a more unsecure group. Interestingly the attacker might also force the use of a stronger group. This could be used in denial-of-service attacks or for amplifying timing side-channels. [1]

Vanhoef and Ronen proposed a mitigation to this attack. Including a bitmap of the supported groups in the 4-way handshake would allow for an AP to detect if a downgrade attack took place and if so, abort the handshake. [2] However as this is not backwards compatible with WPA3, the current security consideration offered by the Wi-Fi alliance is to only allow the use of suitably strong groups by the AP [5] making it impossible for an attacker to gain an advantage by choosing the weakest group.

7 High Overhead of Dragonfly Handshake

The number of operations that Dragonfly's hash-to-element method requires is an order of magnitude more than alternative methods. This high overhead is caused by a defence against timing side-channel attacks. [1]

The designers of Dragonfly did realize that an adversary can abuse this high overhead by spoofing commit frames to perform a DoS attack. To defend against this an anti-clogging mechanism was added to SAE. The client must reflect a simple cookie sent by the AP before the AP processes the client's commit message. This means that an adversary can only use it's real MAC address in commit messages which in allows for throttling of connections based on the address. [1]

However as it is trivial to change a MAC address of a network device. Therefore this defence is ineffective, as the attacker can simply keep changing the MAC address to avoid being throttled. [1]

Vanhoef and Ronen were able to use a 700MHz CPU and a Wi-Fi dongle to attack a professional AP with a 1200 MHz CPU. By spoofing 70 commit exchanges per second the AP's CPU usage reached 100% while the CPU usage of the attacker was only 14.2%. This either created long delays or completely stopped new clients from connecting to the AP. This attack was done using curve P-256 which all AP's must support. Therefore an effective DoS attack can be carried out against any WPA3 network. The effectiveness of this attack is illustrated in figure 3, which also provides the total airtime used by the DoS messages. [1]

One proposed countermeasure is to modify the Dragonfly handshake such that the password element is independent of the peer's identities, this would allow the password element to be calculated once and reused in all handshakes. A WPA3 compatible solution would be to unprioritize the hash-to-element calculation. This will mean that the DoS attack will only stop new clients from connecting but it will not hinder other communication [1]. The Wi-Fi Alliance has also adopted this as their official security suggestion [5].

Another aspect of the high overhead is that some lightweight WPA3 devices will probably not fully implement the defences against the timing-attacks, as it simply too costly for the device. [1]

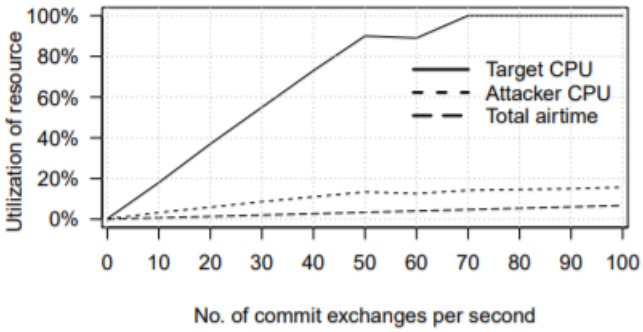

Figure 3: Comparison of target's and attacker's CPU usage and the total possible airtime used with regards to the number of messages sent. [1]

8 Side-Channel Attacks

Vanhoef and Ronen also discovered multiple side-channel attacks against the WPA3 which leak some information about the passphrase, making it somewhat feasible to perform online/active brute-force attack against it [1].

The hash-to-element function used for the MODP groups contains a possible timing leak. For most groups used the probability of a timing leak happening is negligible, however there are some groups for which the probability is notable (up to 47,01%). The time this function takes to run is influenced both by the passphrase and MAC address of the identities (client and AP). Spoofing MAC addresses for the client can be used to amplify the attack to gain even more information about the passphrase. [1]

The so called brainpool curves used in some elliptic curve variants of the Dragonfly handshake were also shown to be vulnerable. However due to the existing methods that mandate executing extra iterations this leak was non-trivial to exploit. Nevertheless this too leaks some information about the passphrase. [1]

To mitigate the attacks two approaches can be taken. Unsecure MODP groups should not be allowed by the APs. For brainpool curves the existing timing side-channel attack mitigation methods should require even more iterations. Similar guards that require a constant number of iterations could be added to the MODP hash-to-element method. An even better defence would be to exclude the MAC addresses from the has-to-element functions. This would only leak two bits of the password on average. [1]

In the figure 4 the practical implications of these vulnerabilities can be seen.

9 Conclusion

WPA3 completely eliminates the possibility of offline dictionary attacks. In theory it could make brute-force attacks against the passphrase almost completely unfeasible, however due to the multiple side-channel attacks some implementations of WPA3 are still somewhat vulnerable to online brute-force attacks. Even though the Wi-Fi alliance has provided some suggestions on how to mitigate these attacks, researchers have argued that the variant of the Dragonfly handshake used in the WPA3 is inherently too difficult to implement securely.

Group / Dictionary	Dictionary Size	$ for MODP 22 Brainpool 28	$ for P-256
RockYou [20]	$1.4 \cdot 10^{7}$	$2.1 \cdot 10^{-6}$	$4.4 \cdot 10^{-4}$
HaveIBeenPwned [44]	$5.5 \cdot 10^{8}$	$8.0 \cdot 10^{-5}$	$1.7 \cdot 10^{-2}$
Probable Wordlists [12]	$8.0 \cdot 10^{9}$	$1.2 \cdot 10^{-3}$	$2.5 \cdot 10^{-1}$
8 Low Case	$2.1 \cdot 10^{11}$	$3.0 \cdot 10^{-2}$	6.5
8 Letters	$5.3 \cdot 10^{13}$	7.8	$1.7 \cdot 10^{3}$
8 Alphanumerics	$2.2 \cdot 10^{14}$	$3.2 \cdot 10^{1}$	$6.7 \cdot 10^{3}$
8 Symbols	$4.6 \cdot 10^{14}$	$6.7 \cdot 10^{1}$	$1.4 \cdot 10^{4}$

Figure 4: Cost of brute-forcing a password using side-channel leaks. Costs for different groups and dictionaries is added. [1]

WPA3 does not provide a complete fix against the Key Renegotiation Attacks discovered in 2017.

WPA3 is also rendered vulnerable to a new DoS attack. However as DoS attacks are also possible against WPA2 this does not strictly make the WPA3 protocol worse in comparison. Instead it could be a sign that the WPA3 standard was not put together thoroughly enough.

Even though WPA3 still contains multiple vulnerabilities, none of these vulnerabilities make it less secure than WPA2. As WPA3 provides forwards secrecy it is definitely an upgrade over WPA2 security wise. However WPA3 can be too cumbersome for lightweight devices to implement securely. As this standard has not yet been widely adopted, hopefully the Wi-Fi alliance takes this opportunity to provide a new standard which fixes those issues, but until they do WPA3 is the most secure way to use Wi-Fi.

References

[1] Mathy Vanhoef and Eyal Ronen. *Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-wpd.*
https://eprint.iacr.org/2019/383.pdf

[2] Mathy Vanhoef and Frank Piessens. *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2.*
https://papers.mathyvanhoef.com/ccs2017.pdf

[3] Robert Moskowitz. *Weakness in Passphrase Choice in WPA Interface.*
https://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html

[4] Christopher P. Kohlio and Thaier Hayajne. *A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3.*
https://www.mdpi.com/2079-9292/7/11/284/pdf

[5] Wi-Fi alliance. *WPA3™Security Considerations Overview.*
https://wpa3.mathyvanhoef.com/WPA3_Security_Considerations_20190410.pdf