Evolution of Wireless Security

Nils Lorentzen, Leander Seidlitz*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: nils.lorentzen@tum.de, seidlitz@net.in.tum.de

***Abstract*—Wireless connections have become one of the most commonly used connection types, and securing connections over an open medium has a long history. A lot has changed since the beginning of WEP in 1997 to today's standard WPA3, released in 2018. While WPA2 was the prevailing standard for a significant period, its vulnerabilities grew to a critical point, necessitating the development of a new, more robust standard. This paper focuses on the transition from WPA2 to WPA3 and gives an overview of their design principles and reasons for change. There is also a short look at other additional improvements to wireless security made for open networks.**

***Index Terms*—WPA2, WPA3, Wireless Networks, Security**

1. Introduction

Millions of people use the Internet over a wireless connection at work, home, or while travelling daily. In an industrial nation, almost everyone uses a mobile phone or a laptop in their daily lives. Without proper protection, it is no problem to read, intercept, and change messages sent over a wireless connection because it is not a closed system, and theoretically, anyone can access the used frequencies. The IEEE committee introduced different security protocols to ensure the confidentiality and integrity of those messages, starting with the Wired Equivalent Privacy protocol (WEP) in 1997. Because of serious vulnerabilities, it was replaced by the first Wi-Fi Protected Access protocol (WPA). WPA was introduced in 2003 with the IEEE 802.11i [1] standard as a temporary solution because of the weak Rivest Cipher 4 (RC4) encryption algorithm used in WEP and was soon updated to WPA2 in 2004 [1]. Over the years, there were some amendments to this standard, but until 2018, when WPA3 was announced, no newer version existed. WPA2 is still widely used today, but it definitely has weaknesses, some of which were discovered over the years. This is why WPA3, the newer standard, became increasingly necessary, as extensions developed to counter vulnerabilities were just optional. To understand the main changes from WPA2 to WPA3, we will first examine the basic protocol procedure of WPA2 and then examine what changed with WPA3. Afterwards, we will also look at the weaknesses of WPA3 [1], [2].

2. Wi-Fi Protected Access 2 (WPA2)

The WPA2 protocol introduced in the IEEE 802.11i-2004 standard establishes a secure connection to an access point and is meant to provide confidentiality, integrity, and mutual authentication between a device and the access point. The big problem with WEP and WPA was the weak RC4 encryption algorithm, which was shown to have multiple vulnerabilities. WPA was only a temporary solution to address this critical weakness of WEP and it used a longer key size for the RC4 stream cipher. This changed with WPA2, which implements the AES-CCMP encryption algorithm as defined in the IEEE 802.11i-2004 [1] standard. AES-CCMP is based on the Advanced Encryption Standard and uses the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, which is computationally more demanding than RC4. So much more demanding that new hardware was needed for access points. This was ultimately why WPA with RC4 and a longer key size exists at all [1].

2.1. Key Management

According to the IEEE standard, the access point is referred to as the authenticator, and the client is referred to as the supplicant. These definitions will also be used here. WPA2 does not use a single key to achieve the desired security goals. Instead, two key hierarchies are defined, one for each of the following scenarios. There are two scenarios for communicating in wireless networks, either directly via unicast between the supplicant and authenticator or as a broadcast/multicast to the network. WPA2 also uses two keys for these two scenarios. For unicast messages, the Pairwise Transient Key (PTK) is used. As the name states, this key is pairwise, unique between the authenticator and a supplicant. At the top of the unicast key hierarchy stands the Pairwise Master Key (PMK). This 256-bit key needs to be known by the authenticator and supplicant before the four-way handshake explained in Section 2.2 can be done. This can be done in different ways, such as using a Password-Based Key Derivation Function, in this case PBKDF2, to derive the PMK from the passphrase. The PTK is not directly used to encrypt or decrypt messages after the handshake. Instead, it is split into different parts for different tasks. The first 128 bits of the PTK will be the Key Confirmation Key (KCK), which provides data origin authenticity for handshakes. The following 128 bits will be the Key Encryption Key (KEK), which encrypts handshake messages and provides confidentiality. The following 128 bits will finally be the Temporal Key (TK), which is then used to encrypt and decrypt messages after the handshake. The other type of key used is the Group Temporal Key (GTK), shared between all supplicants and the authenticator. The

 doi: 10.2313/NET-2024-09-1_14

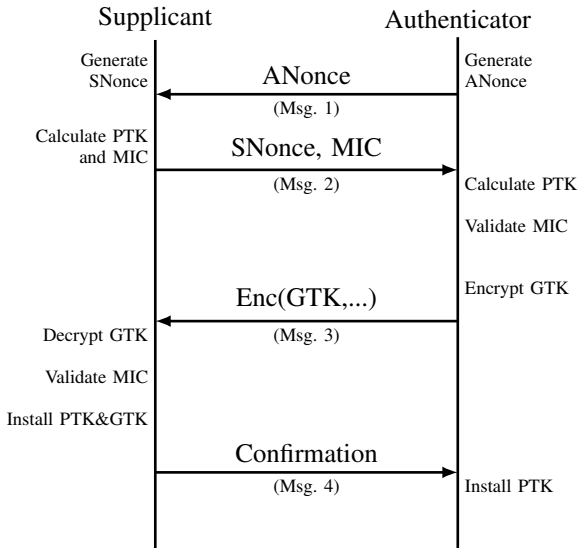

Figure 1: Short diagram of the four-way handshake [1]

GTK is derived from the Group Master Key GMK, a cryptographically secure random number generated by the authenticator. It makes sense to reinitialize the GMK after a specific time interval and redistribute a new GTK to all supplicants. This can be done via a separate simple group key handshake. PTK and GTK are distributed during the four-way handshake, further explained in Section 2.2 [1].

2.2. Four-Way Handshake

Before the four-way handshake starts, the supplicant sends an association request to the authenticator, who then sends an association response. Now, both participants generate a cryptographically secure nonce. The authenticator starts the handshake by sending his Authenticator Nonce (ANonce) to the supplicant. This first message and the following messages can be seen in Figure 1. After receiving the ANonce, the supplicant can compute the PTK using both nonces, the PMK and the MAC addresses of both participants. The nonces are used to protect against replay attacks. To ensure that no one interferes with the first two messages, the supplicant computes a message integrity code (MIC). This is where the KCK is used. The second message's primary information is the SNonce, which is integrity-protected by the MIC. The authenticator can now also compute the PTK and validate the MIC. If a third party changes the ANonce or SNonce in the first or second message, this will be detected at this point. Essentially, both supplicant and authenticator now have a shared key and can communicate encrypted. The only thing missing is that the authenticator sends the GTK to the supplicant and the handshake can be finished with a last confirmation message of the supplicant [1].

2.3. Security Considerations

Especially with wireless communication compared to wired communication, it is easy to intercept or eavesdrop on messages, so it is crucial that the protocols used offer as little attack surface as possible. For example it is possible for anyone to sniff the four-way handshake and this alone is no problem but can get one if the station listening is malicious and also has access to the pre-shared secret (in most cases a passphrase) used for the network. With this extra information, it is also possible for the attacker to compute the exchanged keys. Even if the attacker is too late to eavesdrop on the handshake or has no access to the pre-shared secret, there are still open attack vectors, as shown in the following.

2.3.1. Deauthentication Attack. One uncomplicated attack on a wireless connection secured by WPA2 is the deauthentication attack. Management and control frames are not part of the payload in these connections and are, therefore, not encrypted nor authenticated. Usually, a deauthentication frame is sent by either the supplicant or the authenticator to indicate that the connection should be closed, but it is easy for an attacker to spoof the source MAC address and send this frame repeatedly to either the authenticator or the supplicant [1], [3].

2.3.2. KRACK Attack. The Key-Reinstallation Attack (KRACK) was first demonstrated in 2017 by Vanhoef and Piessens in [4] and raised major concerns about the security of WPA2. This attack focuses on the four-way handshake and it works by tricking the victim into reusing replay counter values with the same key. After installing a key through the regular four-way handshake, the replay counter value starts at zero and increases after sending messages. The attack concept is to trick the victim into installing the same key as before and reinitializing the replay counter to zero. This enables the attacker to read all sent packets even with AES-CCMP in use [4], [5].

2.3.3. Handshake Capture Dictionary Attack. By eavesdropping on a successful handshake, an attacker can use this technique to obtain the passphrase used by the authenticator. The attack is based on an offline dictionary attack. It exploits the fact that both nonces are sent in plain text and are the only random source for calculating the PTK. After both nonces have been intercepted, it is possible to force the passphrase and validate the current attempt with the MIC sent in the second message. Therefore, this can be performed as an offline attack, making the brute force and dictionary attempt possible [6].

3. Wi-Fi Protected Access 3 (WPA3)

Over the years, amendments have been made to the original IEEE 802.11i standard to eliminate vulnerabilities. However, these changes were voluntary and must be used by both communication partners. Therefore, the Wi-Fi Alliance introduced WPA3 in 2018, just one year after the publication of the KRACK attack method. This version aims to eliminate all known vulnerabilities of the old standard, including the previously mentioned KRACK and deauthentication attacks. There are different variants of WPA3, for example, WPA3-Enterprise only mode or WPA3-Personal only mode, which we will focus on here because of simplicity. The Enterprise mode is mainly used for bigger company and institutional networks while the Personal mode is also deployed in many private households [6], [7].

3.1. Simultaneous Authentication of Equals

With several security improvements, WPA3 adds another layer to the initial key exchange handshake. The technique used is called Simultaneous Authentication of Equals (SAE), which Dan Harkins first introduced in 2008 [8]. SAE Public Key (SAE-PK) is the extended version used in WPA3 to counter attacks like the "evil twin AP" attack [7] and also the previously mentioned KRACK attack. With this extension, an asymmetric cryptography key pair also authenticates the access point. SAE is a version of the Dragonfly key exchange that is based on the discrete logarithm problem and, therefore, works with prime modulo groups or elliptic curve groups. In comparison to integer exponentiation modulo a prime problems are elliptic curves still harder to solve. Therefore, the keys for elliptic curves can be smaller and still be considered secure. In contrast to the regular four-way handshake, the passphrase is not directly used to compute the PMK. Instead, the passphrase is converted to a specific elliptic curve similar to a hash function, which is then used to compute a password element (PE). To increase the entropy in this equation, an increment counter, supplicants, and authenticators' MAC addresses are used in an iterative procedure to determine the PE. The increment counter is increased in each iteration, and then a new hash is computed for all factors. This hash is then used as x and if there exists a solution for y in (1), the coordinates (x,y) will be used as PE in the following handshake. a,b and p are factors of the specific elliptic curve that is used [6], [8], [9].

$$y^2 = x^3 + ax + b \mod p \tag{1}$$

Now, this PE will be used in the dragonfly handshake, which outputs an initial PMK that can then be used for the normal four-way handshake [6].

The way this dragonfly handshake is constructed it is not computationally feasible to reconstruct the PMK after learning about the passphrase. So this protocol is perfect forward secret, which was not the case with standard WPA2 [6], [9]. Because of the extra entropy added in this procedure, offline dictionary attacks are no longer possible as well [9].

3.2. Protected Management Frames

Another issue with WPA2 was the relatively easy deauthentication attack 2.3.1, which is one reason why in 2009 the amendment IEEE 802.11w [10] was made where the Protected Management Frames (PMF) protocol was introduced. The usage of these frames became mandatory for WPA3. IEEE 802.11w protects specific frames as Robust Management Frames (RMF). These are disassociation, deauthentication and robust action frames. So the amendment itself is named Protected Management Frames while the frames itself are part of the Robust Management Frames. PMF uses the Broadcast Integrity Protocol (BIP) to guarantee data integrity and replay protection. Essentially, a MIC is computed not only over the data frames but also for management frames [6], [10], [11].

Protected Management Frames protect against deauthentication attacks, if an attacker sends an unprotected deauthentication request the receiving station will no longer directly deauthenticate the device but will temporarily reject this request and also send a Security Association (SA) query back. If the original station that the attacker wanted to deauthenticate is in the network, it will be able to answer this SA query with the correct key. Otherwise, the SA query will timeout, and it can be assumed that the original station is either already disconnected or no longer able to use the key and needs to re-associate [6], [10], [11].

3.3. WPA3 Security Considerations

Even though WPA3 was intended to eliminate all vulnerabilities of WPA2, this is not the case. Several attacks were found on different WPA3 mechanisms, including the previously mentioned Protected Management Frames and Dragonfly key exchange.

3.3.1. Deauthentication Attack on PMF. In a scenario with one supplicant and one access point in a unicast communication channel it is possible to deauthenticate these two peers. To achieve this, "a large number of spoofed unprotected unicast deauthentication frames" [11] are sent to both peers. This means that the supplicant and access point will start sending SA queries to the other peer. As soon as the access point sends the SA query to the supplicant it ignores any SA query coming from the supplicant. This will then lead to a timeout on the supplicant's side and cause a disassociation [11].

3.3.2. Dragonblood Attacks. In April 2019, M. Vanhoef, who also participated in the KRACK attack [4] and E. Ronen published a paper [9] about multiple attack vectors on the dragonfly handshake. The so-called Dragonblood attacks contain, among others, timing side-channel, downgrade and denial-of-service attacks. For example, it is enough to know the SSID of the network and be close enough to the victim to perform a downgrade attack by just advertising a WPA2-only network. During the four-way handshake, the downgrade attack will be detected by WPA2, but with the information gathered through authenticated four-way handshake messages, a dictionary attack becomes possible [9].

3.4. WPA Conclusion

Keeping wireless connections secure is not a Task which is done at some point. Over the time someone will eventually come up with an idea to attack the protocols in place and this is also the case for WPA3 as well as it was the case for WPA2. Protocols have to evolve and adapt constantly to vulnerabilities as well as other factors that may change the way wireless connections work. WPA3 may not be perfectly secure today but for most cases the attacks on it are hard enough to not be really worth it.

4. Opportunistic Wireless Encryption

WPA3 is not the only protocol currently available to secure wireless connections, in a different use case a different approach might be better. For example in todays

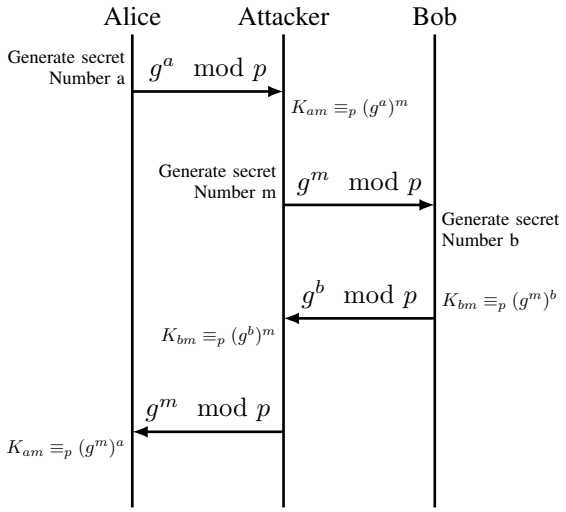

Figure 2: A Diffie-Hellman key agreement man in the middle attack with publicly known integer prime numbers g and p. K_{am} and K_{bm} are the resulting DH-keys between Alice/Bob and the Attacker. They can be used as seed for a proper key derivation function [14].

world it is common to have internet access almost everywhere at public places like restaurants or airports offered by unprotected wireless networks. It is just not practical enough for large public spaces to distribute shared secrets to everyone, and this would also not be convenient enough to attract customers. The only possible way to do this without much effort is to publicly advertise the passphrase to the network. This technique became popular over the years and as explained in 2.3 it is possible to completely bypass this which is even worse because users get a wrong impression of security in their connection to the internet. So a way to protect these kinds of connections is needed and a one way to improve this is called Opportunistic Wireless Encryption. OWE was standardized in 2017 with RFC8110 [12] and is currently not part of the WPA3 standard [7] but was introduced as the Wi-Fi Enhanced Open certification by the Wi-Fi Alliance in 2018 [13]. Essentially, a Diffie-Hellman key exchange is done, and the resulting shared secret is used in the four-way handshake. This way no public passphrase is needed and every participant has an unique shared secret with the access point but it can not be guaranteed that this is the correct access point. Plain Diffie-Hellman does not provide any authentication [12].

OWE is a replacement for unencrypted communication and can contribute to a more secure connection. The end user does not have to actively participate in this protocol, which maintains the convenience of an open connection. However, the problem is that an active man in the middle attack on the Diffie-Hellman key exchange is still possible. This can be seen in Figure 2. This is why it does not provide any type of authentication, as said in Section 4. The only things protected by OWE are packet integrity, confidentiality, and authenticity between two peers. Which peer is really on the other side of the connection is not known. This is where the Opportunistic approach comes from. The protocol hopes that on the first connection the correct access point is chosen and therefore a secure connection can be established. A proper end-to-end connection on a higher layer should still be established to mitigate the security risks in an open connection [12].

5. Conclusion

For many years, WPA2 was the newest standard in terms of wireless security. It was constantly updated and improved, but the use of these amendments was not mandatory. Because of this, a new standard is necessary at some point, and with the KRACK attacks described in Section 2.3.2, this point was reached. WPA3 was introduced and includes new features and techniques already used as amendments to the WPA2 standard, which has now become mandatory to use in WPA3. The goal is to eliminate all WPA2 vulnerabilities. The KRACK attack is countered by a new extended handshake, the Dragonfly handshake. Nevertheless, just one year after its release, the Dragonblood attacks revealed significant weaknesses in this handshake. Another new security mechanism is the Protected Management Frames, which are designed to prevent deauthentication attacks, among other things. It took more time to break these, but eventually, in 2022, Lounis et al. [11] published several ways for deauthentication attacks on Protected Management Frames. Overall, WPA3 is harder to attack than WPA2, which is an improvement, but it is still vulnerable as shown in Section 3.3. Achieving a high safety standard requires much work and constant further development. Solving all these vulnerabilities is a hard task, but as of today WPA3 is the newest standard regarding wireless security and has solved many vulnerabilities of the past versions and therefore should be used. It is uncertain for how long WPA3 will be the newest standard around. Maybe sometime in the future, WPA4 will be necessary because some vulnerabilities can not be solved with an amendment to the WPA3 standard or a completely new standard will be introduced to accomplish the goal of securing wireless connections to the Internet. One example of an independent addition to wireless security in open networks is Opportunistic Wireless Encryption, even though it was discussed to be included in the WPA3 standard. Of course, this protocol has its own problems and is no replacement for a proper authentication and encryption method. This is one of the goals of future research in this area and it is important to keep updating security standards because also the attacks on wireless networks are constantly evolving.

References

[1] "Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements-part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications: Amendment 6: Medium access control (mac) security enhancements," *IEEE Std 802.11i-2004*, pp. 1–190, 2004.

[2] "Ieee standard for wireless lan medium access control (mac) and physical layer (phy) specifications," *IEEE Std 802.11-1997*, pp. 1–445, 1997.

[3] C. Mitchell and C. He, "Security analysis and improvements for ieee 802.11 i," in *The 12th Annual Network and Distributed System Security Symposium (NDSS'05) Stanford University, Stanford*, 2005, pp. 90–110.

[4] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 2017, pp. 1313–1328.

[5] C. Cremers, B. Kiesl, and N. Medinger, "A formal analysis of {IEEE} 802.11's {WPA2}: Countering the kracks caused by cracking the counters," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 1–17.

[6] C. P. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for wi-fi and wpa3," *Electronics*, vol. 7, no. 11, 2018.

[7] W. Alliance, "Wpa3 specification v3.3," 2024.

[8] D. Harkins, "Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks," in *2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008)*. IEEE, 2008, pp. 839–844.

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

[10] "Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 4: Protected management frames," *IEEE Std 802.11w-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, and IEEE Std 802.11y-2008)*, pp. 1–111, 2009.

[11] K. Lounis, S. H. H. Ding, and M. Zulkernine, "Cut it: Deauthentication attacks on protected management frames in wpa2 and wpa3," in *Foundations and Practice of Security*, E. Aïmeur, M. Laurent, R. Yaich, B. Dupont, and J. Garcia-Alfaro, Eds. Cham: Springer International Publishing, 2022, pp. 235–252.

[12] D. Harkins and W. Kumari, "Rfc 8110: Opportunistic wireless encryption," USA, 2017.

[13] W. Alliance, "Opportunistic wireless encryption specification," *Specification v1.1*, 2020.

[14] L. Lizama and J. R., "Non-invertible public key certificates," *Entropy*, vol. 23, p. 226, 02 2021.