A Survey of WiFi Security Protocol: WPA3

Ayan Patel
Computer Science
California Polytechnic State University
San Luis Obispo, CA
apatel60@calpoly.edu

***Abstract*—Wireless devices are becoming more popular. WiFi is one of the most common wireless standards used. This paper looks at the security protocols in WiFi. In particular, it looks at WPA3, comparing it with previous protocols including WPA2 and identifying what security goals are met. We take a look at different vulnerabilities in WPA3. Some attacks used in WPA2 are resolved in WPA3 due to the use of the Dragon-fly handshake. However, there are still new Dragon-blood vulnerabilities in WPA3 that take advantage of the algorithm used in the Dragon-fly handshake. WPA3 is an improvement to WPA2, but is still vulnerable so it does not meet all our security goals.**

I. Introduction

Wireless devices, including IoT devices, are becoming more common in households and they all need a way to communicate with each other and with the internet. Many IoT devices use other proprietary protocols to communicate amongst each other but at least one central station must be connected to the internet through a wired or wireless connection [6]. Most of these devices contain private information that should be encrypted over the network. The increase in IoT devices requires a wireless standard that can allow these devices to communicate securely end-to-end in a network.

WiFi is a commonly used protocol to allow such connections. WiFi is also very popular and the majority of users have a router and access point already setup in their house. WiFi can be used with two frequencies – 2.4GHz and 5GHz. Within these frequencies there are different channels that can be used because if two routers broadcast over the same channel they create interference [6].

Over the years, WiFi has used security protocols including WEP, WPA, and WPA2. These protocols, especially the Wireless Protected-Access protocols, are currently widely used on wireless networks. There are still some networks that do not use any encryption to allow easy access for the public, but this means that the information is open for everyone to see and susceptible to man-in-the-middle attacks.

WPA2 is not secure anymore due to several vulnerabilities [8]. WPA3 was recently introduced as is being adopted as the new WiFi security protocol. This paper aims to look at the security features of WPA3 and the Dragonfly Handshake and how they are an improvement from WPA2. We take a look at different vulnerabilities in WPA3 and potential mitigations to these attacks.

II. Security Goals

A. Authentication

Both the receiver and sender should be verified before data is transferred between them. [9]

B. Confidentiality

Only authenticated entities should be able to interpret the message or data. Usually done using encryption. [9]

C. Integrity

The content of the data should not be modified in transit between the sender and receiver. [9]

D. Availability

Services should be available to the user and provide a reliable connection. [9]

III. Previous Security Protocols

A. WEP

Wired Encryption Privacy (WEP) attempted to achieve confidentiality, availability, and integrity [9]. WEP uses the RC4 algorithm for encryption. RC4 is a stream cipher that needs an IV and a shared key to create a key stream. WEP initially used a 40-bit key, which can be broken in a couple hours. This led to the use of 104-bit keys. The main disadvantage of WEP has to do with key management.

WEP does not support mutual authentication, it only authenticates the client, meaning it is susceptible to

rogue AP attacks. WEP uses CRC to ensure integrity. CRC lacks cryptography features meaning that with enough encrypted packets and some plain text, WEP keys can be derived. RC4 tends to repeat IV values due to a IV size of 24 bits, which can be taken advantage of to decrypt messages.

B. WPA/WPA2

WiFi Protected Access (WPA) supports two methods of authentication [9]. The first uses EAP to authenticate users. The second uses a per session key per-device. A pre-shared key is used to generate session keys for authentication and data encryption as shown in figure 1.

For integrity, a new check uses a MIC (Message Integrity Code) which is an 8-bit integrity check. WPA2 uses TKIP or CCMP. TKIP was introduced with WEP and can work with the same hardware. CCMP is considered the optimal solution with AES for secure data transfer and encryption. However, the use of AES requires hardware upgrades from WEP supported routers. TKIP still uses RC4 which has vulnerabilities, so AES is the recommended method of encryption.

C. Problems with WPA2

WPA2 has some problems that led to the creation of WPA3. Open SSIDs offer no protection to the users of the network [7]. This means the data is not encrypted on the network and is susceptible to man-in-the-middle attacks. WPA2-Personal uses a pre-shared key for authentication and encryption. However, anyone with the pre-shared key can snoop communications on the network. In addition, pre-shared keys are susceptible to offline dictionary attacks. WPA2-Enterprise uses usernames and passwords unique to a user. A weakness in the protocol allows for a Key Re installation Attack that allows an attacker to read information previously encrypted [7]. In addition, the Wi-Fi Protected Access Protocol (WPS) is vulnerable to a brute force attack due to the use of a PIN [5].

IV. WPA3 Implementation

WPA3 uses Simultaneous Authentication of Equals (SAE) or Dragonfly Handshake to authenticate and generate a high-entropy master key, PMK, which is then used to do a four-way handshake to generate a session key, PSK, similar to WPA2. This removes the need for a pre-shared key that is identical for all users. The SAE Handshake supports mesh networks by allowing the AP and client to initiate the handshake concurrently [10]. Table I compares WPA3 to WPA2 with regard to security goals.

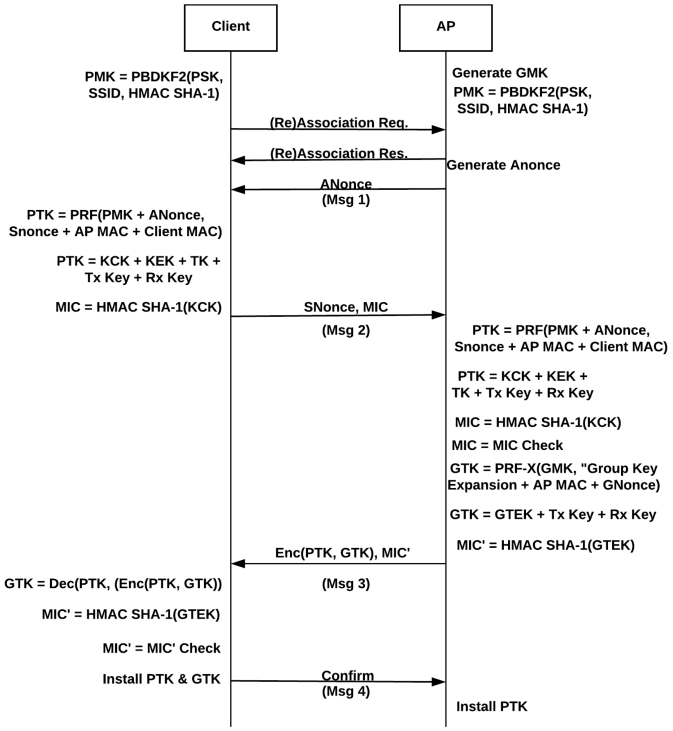

Fig. 1. Four-way Handshake Diagram

TABLE I
Comparison of WPA2 and WPA3 Protocols

	WPA2	WPA3
Encryption	AES-CCMP	AES-CCMP AES-GCMP
Key Size	128-bit	128-bit 256-bit
Authentication	Pre-Shared Key 802.1x with EAP	AES-CCMP AES-GCMP
Integrity	CCMP with AES	SHA-2 BIP-GMAC-256
Key Management	4-way handshake	EC-DH Exchange EC Digital Signature Algorithm

A. Dragonfly Handshake

The Dragonfly Handshake also known as the Simultaneous Authentication of Equals (SAE) is an improvement on the four-way handshake used in WPA2 [8]. The result of the Dragonfly handshake generates a PMK which is then used in the standard WPA2 handshake. The shared password is only used for authentication in SAE, it is not used to generate the PMK.

The PMK is generated using a password element (PE) that is created at the time of session using elliptic curves and logarithmic computations. As shown in Figure 2,

there is several messages sent back and forth between the AP and the station trying to connect to it. A confirmation is needed to verify that the password is correct.

The handshake can be split up into the commit phase and the confirm phase. The client will initiate the handshake by sending its commit frame. The AP will reply using a commit and confirm frame. Then the client sends its confirm frame and completes the handshake [10].

In the commit phase, both the client and the AP pick a random number and a random mask. They calculate the public group element using these values. They send both the scalar and the group element to each other. When the client and AP receive the commit frame from the other, they verify that the received scalar is within a range and the given group element is a valid point on the curve [10]. Due to the nature of the dot product used in the logarithmic computations, it is not possible to find the master key from the element, E, and the password element (PE). This provides forward security.

In the confirm phase, the AP and the client calculate the shared secret point. The x-coordinate of this point is calculated using a hash function to derive the key. The a HMAC is calculated over the handshake summary using the key. The result of this hash is sent to the other participant in its confirm frame. [10] If the value is as expected, the key becomes the PMK. Since interaction with the AP is needed for confirmation, an offline dictionary attack would not work as well.

B. Protected Management Frames

SAE utilizes PMFs between the client and the AP to prevent a malicious third-party from intervening during the process. An extra layer of encryption to each message between the AP and the client allows for a private connection even if the Wi-Fi network is open without a password. PMFs prevent eavesdropping and forging of frames, including system management packets [2].

A Security Association (SA) mechanism is used for extra protection if an unencrypted management frame is used. The SA query prompts the sender to resend the frame within a given time frame. The AP sends an encrypted SA request to the sender and waits for an encrypted response. If the sender is already on the network, they can send the correct response [8].

C. Opportunistic Wireless Encryption

OWE or "Enhanced Open" SSID encryption allows for encryption to be used in open networks used in hotels or cafes. The process relies on Diffie-Hellman Key Exchange to be able to generate a unique key per device [7]. This removes the need of a pre-shared key to connect to the network. OWE with PMFs allows for an added layer of protection, preventing disassociation attacks that force re-authentication with the network. This is an improvement over WPA2 in which open networks were public without encryption.

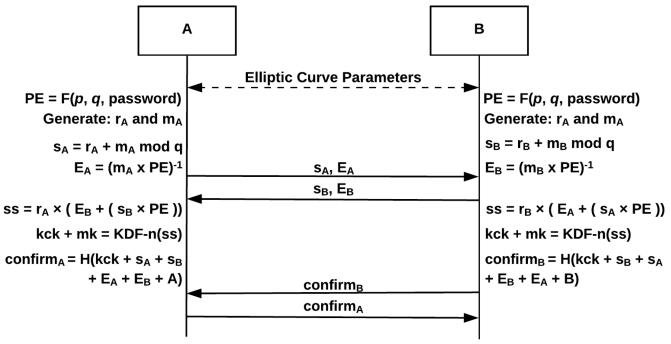

Fig. 2. Dragonfly Handshake Diagram

D. Device Provisioning Protocol

DPP is a replacement for Wi-Fi Protected Access (WPS) which is a vulnerable protocol. DPP allows for provisioning devices including IoT devices, using another device like a mobile phone. DPP consists of bootstrapping, authentication, and network access [5]. DPP protects against eavesdropping, active attacks to add unauthorized devices to the network, and denial of service blocking provisioning. In bootstrapping, entities transfer their public keys. In authentication, PMK and PMKSA are created. Authentication frames are exchanged using the keys. In network access, the devices mutually derive the PMK and PMKID [5]. The network keys are then used to gain access to the network.

V. Vulnerabilities

WPA3 fixed some of the vulnerabilities in WPA2, but is still susceptible to others. There is also a new group of Dragon-blood vulnerabilities that take advantage of down-grade options and weaknesses in the Dragonfly Handshake. The vulnerabilities can be summarized in Table II.

A. De-authentication Attack

WPA3 is protected against de-authentication attacks due to the use of SA queries [8]. If a malicious user spoofs the MAC address of a client and sends an unencrypted de-auth request to the AP, the AP will send an encrypted SA query to the client. It will then wait for a response, but since the malicious user does not have

TABLE II
VULNERABILITIES IN WPA2 AND WPA3

Vulnerabilities	WPA2	WPA3
De-authentication Attack	Susceptible	Protected
Dictionary Attack	Susceptible	Protected
Rogue Access Point	Susceptible	Susceptible
KRACK Exploit	Susceptible	Protected
MITM:ARP Spoofing	Susceptible	Protected
Downgrade Attack	Susceptible	Susceptible
Timing-Based Side-Channel Attack	Susceptible	Susceptible
Cache-Based Side-Channel Attack	Susceptible	Susceptible
Denial-of-Service Attack	Susceptible	Susceptible
Jamming	Susceptible	Susceptible

the encryption key, he/she is unable to respond. Since the AP did not receive the response within a given time, it will not de-auth the client. If the client receives an unencrypted de-auth request, it will send a SA query to the malicious user, who will not be able to respond.

B. Dictionary Attack

WPA3 is protected against the offline dictionary attack due to the nature of the Dragonfly handshake and confirm frames [8]. Even if the attacker captures parts of the handshake, he/she will not have enough information to figure out the PMK. The password element can be found by brute-forcing the password, but due to the way the key is derived from the elliptic curve, it cannot be derived [8]. A PMKID hash dictionary attack will not work either, due to the fact that the PMK is not directly computed from the pre-shared key and it requires AP interaction for a valid active handshake.

C. Rogue Access Point

A rogue access point or an evil twin attack is partially feasible with WPA3. If a client is already connected to the genuine AP, then it is not possible to de-authenticate the client as mentioned above. However, if the client is not yet connected to the AP, then a rogue AP can clone the genuine AP and capture the handshake when it connects to the genuine AP. Then the rogue AP will increase its signal and the client will attempt to connect to it instead. The rogue AP then can obtain the passphrase for the genuine AP by asking the user through a landing page. The adversary can find the PMK, PTK, and MIC by checking against a captured handshake [8].

D. KRACK Exploit

The KRACK exploit, or key re-installation attack, the adversary tricks the victim into reinstalling an already in-use key by manipulating and replaying cryptographic

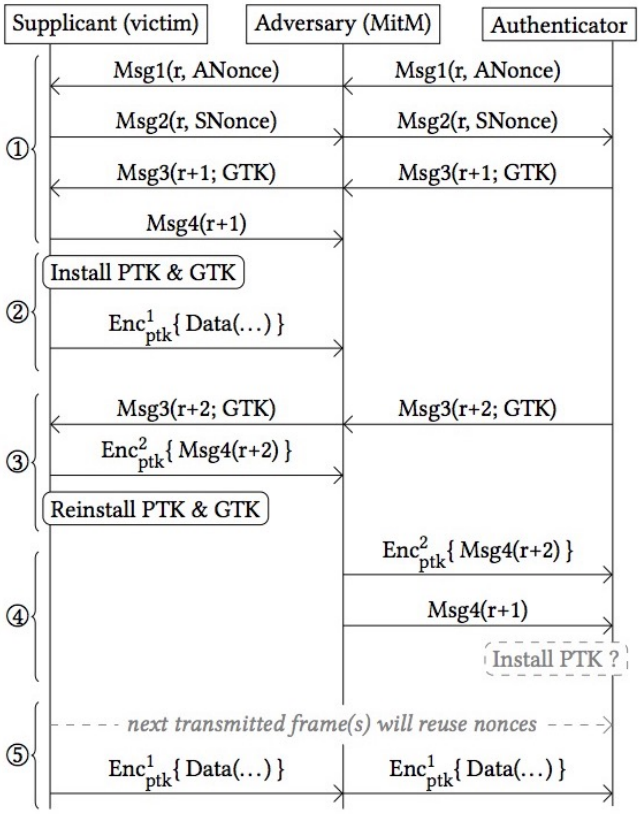

Fig. 3. Key re-installation attack in WPA2

handshake messages. This requires the AP to re-transmit message 3 in the four-way handshake [8] as shown in Figure 3. Reinstalling the key resets the nonce and the sequence number. WPA3 routers with updated security patches will not allow re-transmission of this message, which is critical for this attack to work. Therefore, WPA3 will protect against KRACK attacks.

E. MITM: ARP Spoofing

Man in the Middle Attacks using ARP Spoofing will not work in WPA3 routers. A malicious user would be able to hijack a session by impersonating the client to the AP, however he/she will not be able to impersonate the AP to the client due to client isolation [8]. Client isolation will not allow clients to communicate with each other or know about each other in the network. This feature can be turned on or off depending on the use cases of the router.

F. Downgrade Attack

This attack takes advantage of the backwards compatibility to WPA2 to accommodate older clients. This is a feature in WPA3 called Transition mode [11]. A rogue

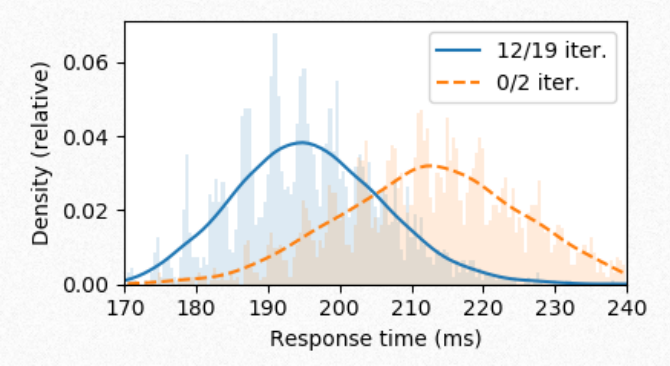

Fig. 4. Brainpool Timing Attack against WPA3

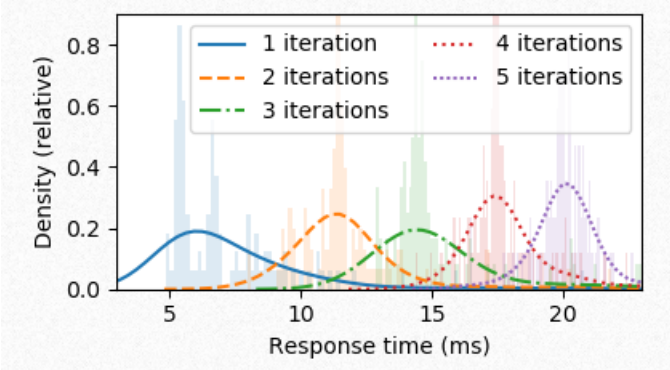

Fig. 5. Timing Attack against EAP-pwd client

access point can force the client to connect to it using WPA2. The captured handshake can be used to find the password using dictionary attacks.

Another variant of this attack takes advantage of security groups in WPA3. A client requests connection with a commit frame with a certain security group. The AP sends a response commit frame either accepting the choice or refusing availability of that group. A rogue AP can force the client to use a weaker security group. Different security groups use different algorithms for creating the key, some of which are less secure than others [11].

G. Timing-Based Side-Channel Attack

Depending on the security group chosen and the algorithm used for deriving the key, timing attacks may be possible. If an AP uses a security group with NIST elliptic curves, no timing data is leaked. However, in other security groups using brain-pool curves or multiplicative security groups modulo a prime, the response time is dependent on the password as shown in Figure 4. A dictionary attack can be used on these groups to leak information about the password [11]. The use of MODP over elliptic curves could be necessary for faster performance depending on use cases. Therefore, this timing attack is a valid method and a current vulnerability in WPA3.

H. Cache-Base Side-Channel Attack

If the attacker is able to measure memory access patterns on the client machine as it creates a commit frame, this also leaks information about the password [11]. The attacker could gain access to the client machine through a web browser running JavaScript. Cache-based attacks can be used to determine if a branch was taken in the first iteration of the password generation algorithm [4]. An offline dictionary attack, or a password partitioning attack, can then be used to compare memory access patterns to the real password.

I. Denial-of-Service Attack

A client machine initiates the Dragonfly exchange by sending a commit frame to the AP. Processing this frame and starting the dragonfly exchange is computationally expensive for the AP. An attacker can send as little as 16 commit frames per second to the AP and overload its CPU usage and potentially prevent other clients from connecting to the AP or slowdown functionality of the AP [11]. A mitigation for this attack requires the use of a processing queue on a separate processor [1]. However, this is not feasible as this is a hardware change, leaving current routers vulnerable.

J. Jamming

Jamming is a method that makes noise on the same frequency as a wireless network and forces it to break and disconnect to clients. Both WPA2 and WPA3 are susceptible to jamming and therefore do not satisfy the security goal of availability. However, jamming does not give the attacker access to the network, but simply prevents users from accessing the network. There are some anti-jamming techniques but they are not practical to use in home routers.

K. Flaws in EAP-pwd

The EAP-pwd protocol also uses Dragonfly internally, providing authentication based on a username and password [11]. It is vulnerable to the same attacks discovered in WPA3. Some of the implementations of EAP-pwd are also vulnerable to invalid curve attacks, letting an adversary completely bypass authentication [11]. Most

implementations were also vulnerable to reflection attacks in which an adversary can reflect the commit and confirm frame back to the server [11].

VI. Mitigations

Most of the vulnerabilities in SAE have to do with the password encoding method. Changing the way the algorithm works by computing the password element offline would prevent some of the timing attacks [10]. Some of the attacks focus on backwards compatibility or weaker algorithms. Forcing clients to connect to the AP with the highest security group and WPA3 would help prevent these attacks. Unfortunately, due to the amount of clients not compatible with WPA3, this may not be possible.

Most of these vulnerabilities, including Dragon-blood, can be mitigated with software security patches and does not require any change in hardware [4]. This means that patching your systems and keeping everything up to date is a good idea. In addition, it is always wise to be cautious when connected to an AP not controlled by you in a public place. Using a VPN to hide and encrypt your traffic is always a good extra precaution [3].

VII. Conclusion

WPA3 is a significant improvement on WPA2. The Dragonfly handshake, or SAE, in addition to the four-way handshake provides extra security and protects against some vulnerabilities in WPA2 involving the pre-shared key. However, WPA3 does still have some security vulnerabilities and is not completely secure. Some of these Dragon-blood vulnerabilities can be fixed through software patches, but this does not rule out all attacks.

WPA3 is still not widely used, but newer routers are now starting to provide WPA3 with SAE capabilities. Clients can use WPA3-Personal using the transition mode. SAE functionality can be added using security patches to client systems. However, WPA3-Enterprise with 192-bit security mode may require new hardware.

It would be interesting to look into IoT devices and their capability of using WPA3. Shortening the length of the transition period and not using weaker security groups would be something to look into as well, due to the downgrade attacks. WPA3 is an improvement over WPA2 however it does not meet all the security goals mentioned earlier. In addition, as WPA3 becomes more widely used, more vulnerabilities and exploits may show up.

References

[1] Wpa3 security considerations overview. 2019.

[2] Wifi alliance security, 2020.

[3] Danny Bradbury. Dragonblood: Data-leaking flaw in wpa3 wi-fi authentication. 2019.

[4] Catalin Cimpanu. Dragonblood vulnerabilities disclosed in wifi wpa3 standard. 2019.

[5] Rowell Dionicio. Wi-fi security improvements. 2018.

[6] Dan Dragomir. A survey on secure communication protocols for iot systems. 2016.

[7] Mike Guy. Wpa3 security improvements. 2019.

[8] Christopher P Kohlios and Thaier Hayajneh. A comprehensive attack flow model and security analysis for wi-fi and wpa3. *Electronics*, 2018.

[9] Abdel-Karim R. Al Tamimi. Security in wireless data networks: A survey paper. 2006.

[10] Mathy Vanhoef and Eyal Ronen. Dragonblood: A security analysis of wpa3's sae handshake. *IACR Cryptology ePrint Archive*, 2019.

[11] Mathy Vanhoef and Eyal Ronen. Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd. In *IEEE Symposium on Security & Privacy (SP)*. IEEE, 2020.