What WPA3 Brings to Wi-Fi with Focus on SAE and OWE: A Review and Explanation of Basic Operations

CWNE Candidate Paper Series

CWNE Paper

By

CWNE candidate Ahmad Mostafa

Introduction

Network Security, a subset or peer of cybersecurity (the literature is divided on the hierarchy of security domains, such as network security, data security, information security, computer security, and cybersecurity), is a very important part in making digital life safer and reducing the risks on our networks, in homes, in enterprises, in healthcare facilities, and in industrial factories. In other words, in all areas of our modern digital life.

Protecting data and user privacy is not an easy thing, we witness new hacking techniques that break security controls and hear of illegal access to data and network resources.

Specific concerns arise with wireless network communication. Wireless is an unbounded medium and it is a popular access technology. These two factors often cause intruders and attackers prefer it as a, typically, easier hack target, but developing authentication and encryption technologies has played a vital role in keeping wireless environments safe so far. New attacks demand new security solutions.

In this paper I will review the new technology of WPA3-Personal only and focus on SAE (Simultaneous Authentication of Equals), which is part of WPA3, and OWE (Opportunistic Wireless Encryption), which is part of Wi-Fi Certified Enhanced Open.

From WPA2 to WPA3 what is the difference:

For more than 15 years WPA2 has played a key role in protecting Wi-Fi well (when correctly implemented), and its techniques and technologies must be evolved to keep pace with the trending attacker methods and techniques.

WPA2 has shown some vulnerability to specialty attacks (like the KRACK attack), offline and dictionary attacks, where the attacker can use a script with common passwords (some dictionaries are in the hundreds of thousands or millions of entries). WPA2-PSK has no internal mechanism to discover repeated active attacks to block the source MAC address (though vendors may implement such an algorithm in a proprietary way). Additionally, the attacker device may be able to change MAC addresses nowadays. Sometimes, flooding the AP with

wrong passwords can overwhelm the AP CPU as it is responsible of doing all the cryptographic operation and this can lead to a total crash, for example, a Denial of Service (DoS).

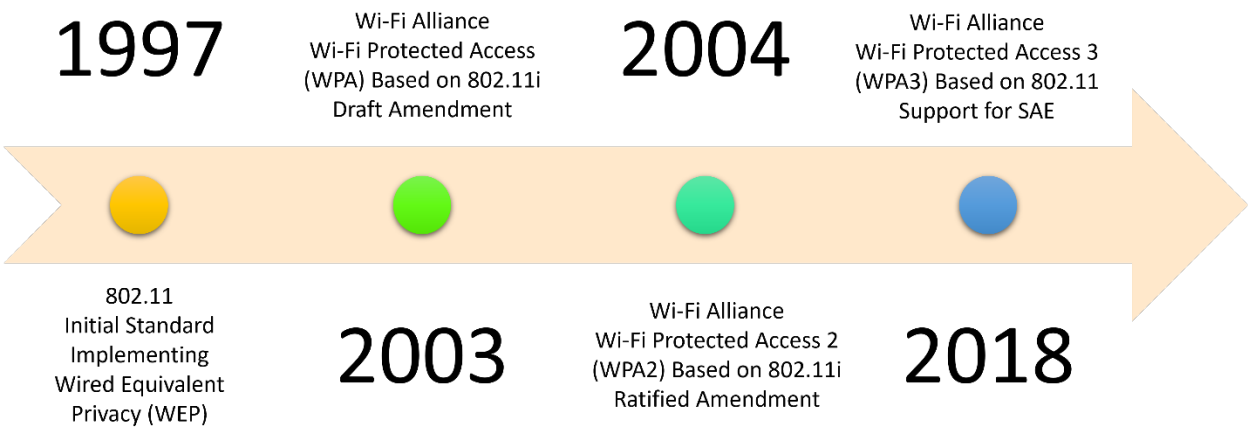
WPA2-PSK passwords have an 8-to-63-character size and, as I mentioned before, using scripts can easily crack it with enough time. With WPA2, it is very important to use a sufficiently long and complex passphrase from which the pre-shared key (PSK) is generated. This helps to thwart dictionary attacks. It should be a completely random passphrase not based on words or common phrases.

Also, other techniques can be used such key reinstallation attack (KRACK) through which the attacker can obtain a valuable information. Vendors have patched their systems to protect against KRACK attacks, but the administrator must be sure to apply the appropriate patches.

WPA2 systems may use older encryption technologies such TKIP (Temporal Key Integration Protocol) which is more vulnerable than the Advanced Encryption Standard (AES) with CCMP. This can result in a weak point allowing the attacker do eavesdrop on the Wi-Fi packets and decrypt them in the worst scenarios.

Security experts recommend using WPA2-PSK AES, which is considered more secure than TKIP with RC4 or AES. Also called WPA2-CCMP as it uses CCMP for key management. CCMP stands for Counter Mode CBC-MAC Protocol, at the same time it can be called AES CCMP which can provide strong encryption technology.

While I have mentioned summaries of WPA2-Personal (or WPA-PSK) in a brief way, this can make the reader aware of the wireless security issues. Next, we will see how WPA3 addresses those issues as a new suite of wireless security methods. Although WPA2-Personal can be heavily criticized, we still have a good level of security provided by WPA2-Personal (when correctly implemented with patches and strong passphrases), and WPA2-Personal will stay in the scene for a while before the time when it is completely replaced by WPA3-Personal. This is normal in the history of security technology transitions.



Timeline of Wi-Fi Security (Image based on Cisco Documentation[1])

At the beginning of this paper, I mentioned that we are focusing on WPA3-Personal, for example, passwords and shared keys only. This decision is because of the high risk that can be realized if the passphrase is discovered, and intrusion of the network occurs. Additionally, the focus is on PSK because WPA2-Enterprise, when correctly implemented, can still provide sufficient security today for all but the most extreme environments.

Many authentication and encryption techniques presented in the Wi-Fi world are preferable to users because they provide easy access to Wi-Fi. However, they still provide a preferred target for hackers to attack. Even with MPSK (multiple PSK), which was introduced in some environments allowing each user to be assigned a unique pre-shared key, it is still a target to crack (though a successful attack will only expose that user's frames or communications).

For these reasons, we need standard technology that contains a protocol to bring more security to networks. This is the purpose of WPA3 – to bring the security features of existing standards (SAE in 802.11 standard and OWE in the IETF standard) to the Wi-Fi world.

[1] https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/wpa3-dep-guide-og.html

WPA3 Technology and OWE

WPA3 is the new technology upgrade of WPA2 and, as I have mentioned, it stands for Wi-Fi Protected Access 3. WPA3 uses a newer technology security protocol and adds new features to make Wi-Fi access simple, robust, and resilient today. The Wi-Fi Alliance says that WPA3 offers the following:

- Uses the latest security methods
- Disallows outdated legacy protocols
- Requires the use of Protected Management Frames (PMF)[2]

WPA3 handles the vulnerability of weak passwords by protecting weak and easy passwords against passive attacks, active attacks, and dictionary attacks, using the new Simultaneous Authentication of Equals (SAE). Attackers can't crack passwords using traditional techniques.

Wi-Fi Enhanced Open can bring safer public Wi-Fi, so attackers must now deal with each session for each user to collect data and use it. Encryption is more advanced and complex as well even though the network is open. Wi-Fi Enhanced Open provides high encryption using Opportunistic Wireless Encryption (OWE) and everyone has their own encryption, and their data are protected.

Therefore, in the remainder of this paper I will focus on two features:

- SAE (Simultaneous Authentication of Equals)
- OWE (Opportunistic Wireless Encryption)

WPA3 SAE

SAE (Simultaneous Authentication of Equals) is a technique used in WPA3-Personal based on what is called the Dragonfly Key Exchange and implements inclusion of Protected Management Frames (PMF), which ensures that key management frames are encrypted as well as data frames. SAE is considered 802.11's newest implemented security access method and it requires a hash

[2] Wi-Fi Alliance definition of WPA3 cited from https://www.wi-fi.org/discover-wi-fi/security

generated key in each authentication process to be unique. This process avoids the use of the same Pairwise Master Key (PMK) all the time.

SAE was introduced in 802.11s with the mesh networking standard amendment but was not implemented in standard user access Wi-Fi – even though it was simply generically specified as a security option[3]. The Wi-Fi Alliance developed WPA3 as a certification to validate that systems appropriately implement SAE in standard access Wi-Fi solutions (for example, Access Points with laptops and other mobile devices connecting with them).

SAE require the Access Points and station to authenticate each time while doing the 4-way handshake, and attackers stay away by the benefit of using cryptographic tools, so password attacks or offline password attacks are less effective or unable to achieve their intended result.

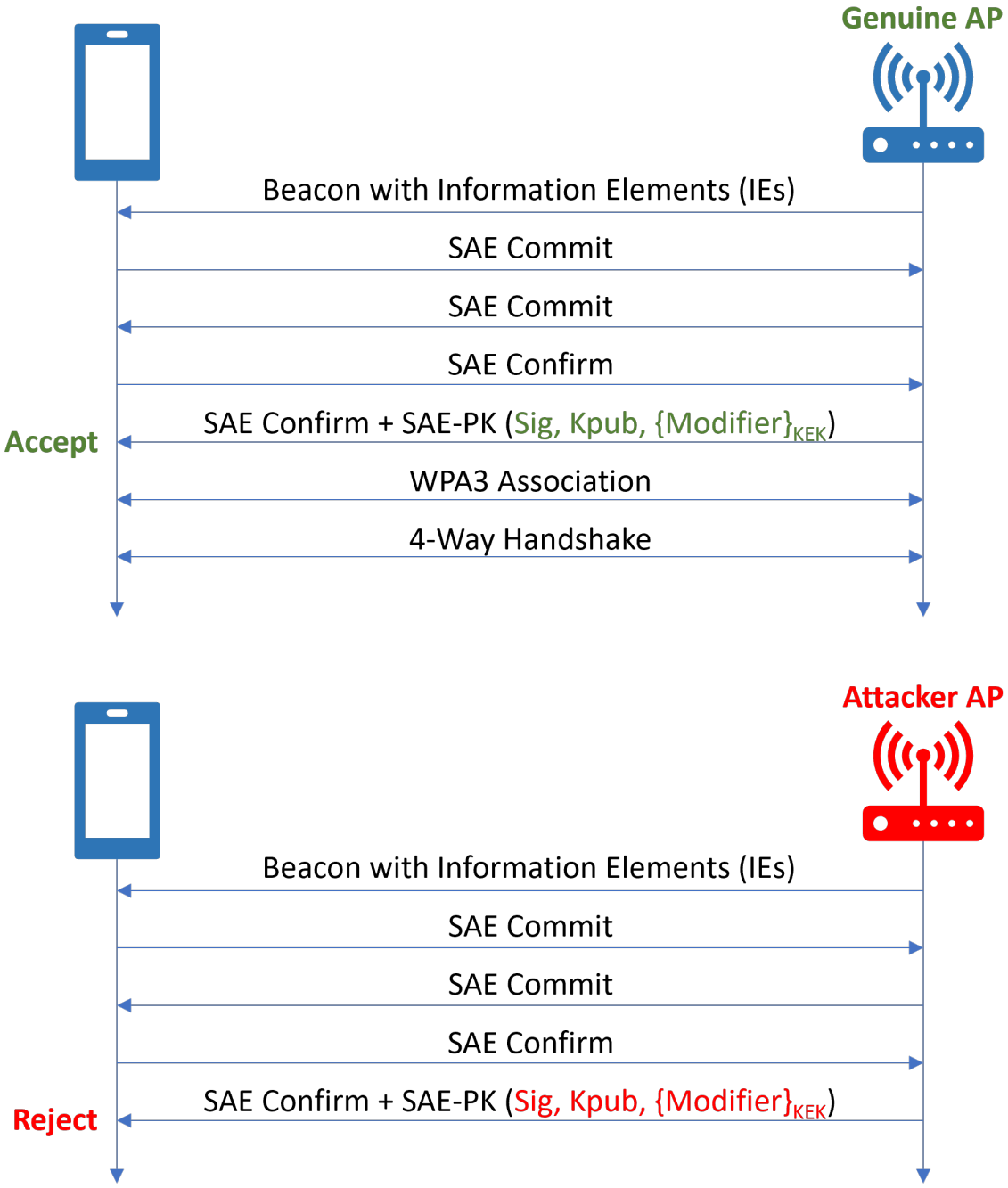
The WPA3-Personal or WPA3-SAE is based on functions of the 802.11 protocol. It can work in two modes:

- WPA3-SAE Mode: is the normal mode to use SAE protection and implement the use of PMF -Protected Management Frames.
- WPA3-SAE transition mode: this mode can handle the capability of the station to use SAE and PMF and, if the station does not support WPA3-SAE, it still can authenticate with the legacy process of WPA2-PSK.

Still another mode used by WPA3-Enterprise 192-bit mode, but because I am focused on Personal only, I will not address that mode further.

SAE authentication uses a signature when the AP sends key information to the station so the station can verify it is valid and can be immune to attackers that cannot mirror that signature. When transition mode is enabled, this enables legacy users to be able to connect and nothing in normal Wi-Fi experience will change, only the security and privacy will enhance for those stations supporting WPA3.

[3] This occurs often as the vendors and engineers often assume that everything in an amendment is limited to "what that amendment is about." In reality, an amendment focused on one specific new capability may add or modify existing general functions to benefit the new capability. These functions are often not constrained to the new capability and SAE in the 802.11s amendment is a good example of this reality.



Genuine AP vs. Attacker AP Connection Processing and Protection[4]

[4] Image recreated based on source: https://www.wi-fi.org/ja/beacon/thomas-derham-nehru-bhandaru/wi-fi-certified-wpa3-december-2020-update-brings-new-0

As you can see, Wi-Fi access with pre-shared key models is continuing to improve. While standard organizations still have their concerns to make Wi-Fi environments safer[5], WPA3 takes a big step forward. But this battle or race between the attackers and the defenders will continue and each challenge need to be addressed, so the game will not end soon as new vulnerabilities are discovered and new security solutions are implemented.

Opportunistic Wireless Encryption (OWE)

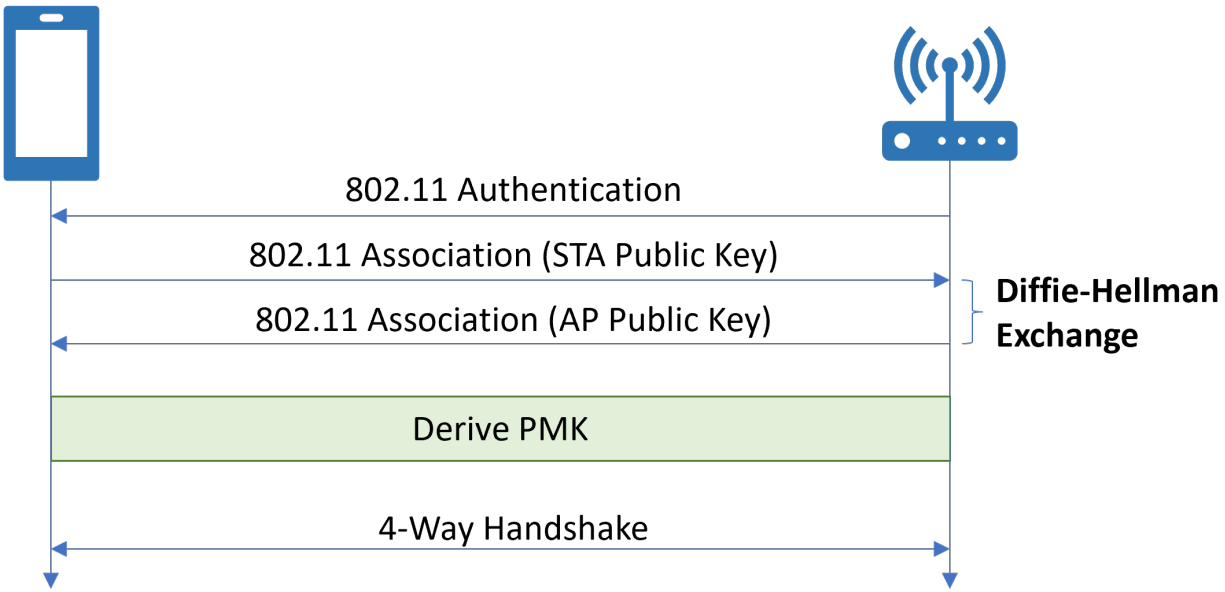
Open network deployments (those using no pre-established credentials), often based on third-party or vendor-specific captive portals, introduce a vulnerability as packets transverse between Access Points and the Stations unprotected (unencrypted). Newer devices can address this issue by using the Wi-Fi Alliance's Enhanced Open which uses OWE (Opportunistic Wireless Encryption). However, it is still optional part of the Wi-Fi security, except for 6 GHz operations, and is commonly implemented on newer devices that support WPA3. Wi-Fi 6E (Wi-Fi 6 in 6 GHz) requires OWE on networks that are "open" and this is driving support for OWE in newer devices that support the 6 GHz band.

OWE performs an unauthenticated Diffie-Hellman (DH) exchange at association time. Stations know that the AP can support OWE based on the AKM (Authentication and Key Management) suite selector field in the AP's Beacon frames. When the station sends an associate request and response exchange, a short-lived key (ephemeral key) is derived via the DH exchange. Then the AP and the station calculate the PMK (Pairwise Master Key) which will be used in the process of 4-way handshake to generate traffic encryption keys.

To enable OWE on your network you need to configure two BSSs with separate Beacons, the first one is configured as Open-Normal for non-OWE capable STAs and acts sometimes as a transition BSS, and the second one is a hidden OWE RSN (Robust Security Network). Clients can discover the SSID of the hidden

[5] This is a battle that will never end if history is any predictor. Historically, all computer security solutions (including network) have had to evolve as new threats and more powerful computers (or the use of millions of computers) have come about. The Wi-Fi engineer must continually focus on security education to ensure proper preparedness for the next big thing.

OWE BSS using the OWE Transition Mode element in the Beacons of the non-hidden SSID. Either active or passive scanning may be used to retrieve the information from the non-hidden AP and to be used to authenticate with the hidden SSID.



OWE Protocol Flow

Before starting the 4-way handshake, the station and AP derive a PMK from the Diffie-Hellman exchange information. After PMK derivation, the traditional 4-way handshake can ensue. And to support mobility the AP and ESS may support caching of the PMK to make the roaming seamless[6].

Status Report of WPA3/OWE

As we go through the migration to WPA3 and/or OWE, we will encounter issues where old access points rely on WPA2 protocols and cannot be software-upgraded. Hardware replacements will be required in such cases. All 802.11ax (Wi-Fi 6 and Wi-Fi 6E) access points from major vendors support WPA3 and

[6] Caching of the PMK is not new, but OWR implementations can take advantage of it as well. This can be useful in larger "open" networks, such as hotels and conference facilities as well as large stadiums offering public Wi-Fi.

many support OWE as well. However, the access points are only a part of the solution. The clients must support it as well to reap the full security benefit. Given that many organizations keep older clients for significant time windows, particularly specialty clients like barcode scanners, the use of transition solutions will be needed for several years.

Conclusion

Data is the gold of this era and protecting data traversing our modern networks in all environments is a huge task, no one wants to be the weak link in this chain, as people before me discussed WPA and WPA2, more people in the future will discuss WPA4[7], or some other named solution, to address security concerns. This loop will not end, as hackers develop new techniques to attack or access data; protectors of data must prepare their systems for more scenarios.

[7] To be clear, WPA4 does not exist at the time of this writing. Given that the gap between WPA2 and WPA3 was well over a decade, it may be the 2030s before we're discussing WPA4, but it (or some other named later solution) is likely to come.