UNDERSTANDING ITS SECURITY GAPS AND EVALUATING THE MOVE TO WPA3

by Iftikhar Javed Khan

Abstract

Today, wireless networks have become the de facto standard for convenient Internet access in homes, retail locations, and corporate offices. Since its introduction in 2004, WPA2 has served as the security standard for wireless communication. While it addressed vulnerabilities in WEP, the ever-evolving threat landscape has revealed weaknesses in WPA2.

These weaknesses in WPA2 have become more apparent, especially after the KRACK attacks in 2017 and the PMKID hash vulnerability in 2018, which have prompted discussions about adopting more robust security measures like WPA3. Though upgrading to WPA3 is recommended, it requires significant infrastructure changes, and management may not fully support the transition. Moreover, WPA3 has also been found to be vulnerable to downgrade and side-channel attacks.

Just as there is no one-size-fits-all approach to wireless network design, the same principle applies to wireless security. As a result, many organizations are left with patching their systems as the most feasible option. When patching, several factors must be considered, such as the vendor's implementation of the standard, the client and AP operating systems, and more.

Despite being the most widely deployed security protocol today, it is estimated that 20–30% of devices using WPA2 remain unpatched.

In this paper, we will discuss the evolution from WEP to WPA2, the advancements made over time, the vulnerabilities inherent in WPA2 modes of operation, and possible remediations.

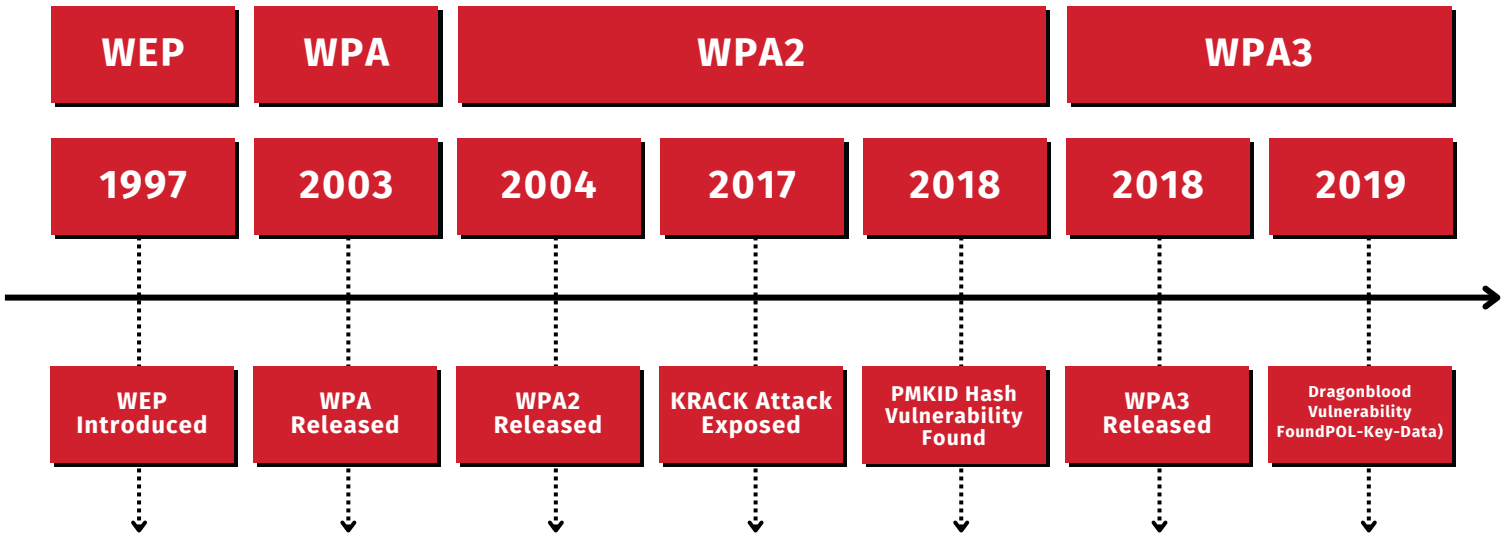

Figure 1 WPA Evolution

WEP

Wired Equivalent Privacy (WEP) was an encryption algorithm leveraged to provide security to users connecting via 802.11 wireless networks. It was designed to enable confidentiality, access control, and data integrity. WEP used RC4 stream cipher and serious security flaws were later identified in the protocol. Some of the main reasons were poor key management, no access point authentication, and WEP key reception. In summary, WEP was considered an obsolete protocol.

WPA2

To address previous security concerns, WPA2 was introduced. The foundation of the WPA2 standard is the 802.11i Robust Security Network (RSN) specification, which defines the following services:

- Authentication: EAP is used to provide mutual authentication and generation of temporary keys between the client and AP.
- Access Control: 802.1X may serve as an authentication function and provides controlled access.
- Privacy with message integrity: Data is encrypted using TKIP or CCMP along with a message integrity code that ensures data is unaltered.

Privacy and Integrity

CCMP was introduced to provide the data confidentiality and integrity protocol. It protects the integrity of both the packet data and portions of the header. CCMP uses a 128-bit session key to encrypt data sent from the client to the AP, ensuring confidentiality, and employs CBC-MAC to verify data integrity.

Encapsulation

CCMP encapsulation involves converting plaintext data, which includes user traffic and a MAC header, into a cryptographic payload (ciphertext). The main steps in this process are as follows:

1. The Packet Number (PN) and other portions of the address field are combined to form a nonce (Random number).
2. The CCMP header is composed of PN and the identifier for the Temporal Key, or KeyID. KeyID is a small value indicating which key must be used to decrypt the received packet.
3. Additional Authentication Data (AAD) is constructed from several fields of the frame header. The goal is to generate a Message Integrity Code (MIC) using AAD, nonce, and actual data.
4. Temporal Key, PN, AAD, nonce, and plaintext data are used as input to CCM to encrypt the data.

Authentication and Access Control

IEEE 802.1X is used to block unauthorized access to a WLAN. It primarily employs the EAP over LAN (EAPoL) protocol for this purpose. It uses controlled and uncontrolled port mechanisms to control access.

- Controlled Port: A logical port that allows access to network resources after successful authentication.
- Uncontrolled Port: A logical port that limits communication before authentication.

Phases of Operation in WPA2

This section outlines the workings of IEEE 802.11 RSN. To provide authentication, encryption, and key management the RSN operations go through the following phases

1. Discovery Phase

The station (STA) uses Beacons and Probe Responses advertised by Access Point (AP) to identify security policies. The STA then analyzes the following elements to associate with the AP and negotiate a cipher suite to be used next. This information is conveyed using the RSN information element (RSNIE) field.

2. Authentication Phase

During this phase, the STA and AP prove their identities to each other. the AP blocks any unauthorized attempt to access network resources using 802.1X.

3.Key Generation and distribution

This final step in the authentication allows the STA and AP to derive keys that make the secure data feasible. This phase includes two types of handshakes to provide integrity and confidentiality.

3.1 4-WAY Handshake

During this handshake, four frames are exchanged between the AP and STA. At the end of this, both the AP and STA have authenticated each other, and data can be encrypted using the keys negotiated during the handshake.

As part of the 4-WAY handshake process, pairwise keys are derived typically for the communication between the client and the AP. These keys form a hierarchy with the master key at the top, and the other keys are derived from it.

There are two possibilities at the top level: either a pre-shared key (PSK) or a master session key (MSK) generated using of 802.1X during the authentication phase.

- Pairwise Master Key (PMK): The PMK is generated using a masker key. If PSK is used then it is used as the PMK. If MSK is used, the PMK is derived from it.
- Pairwise Transient Key (PTK): The PTK is generated using the PMK, and it is a combination of three keys.

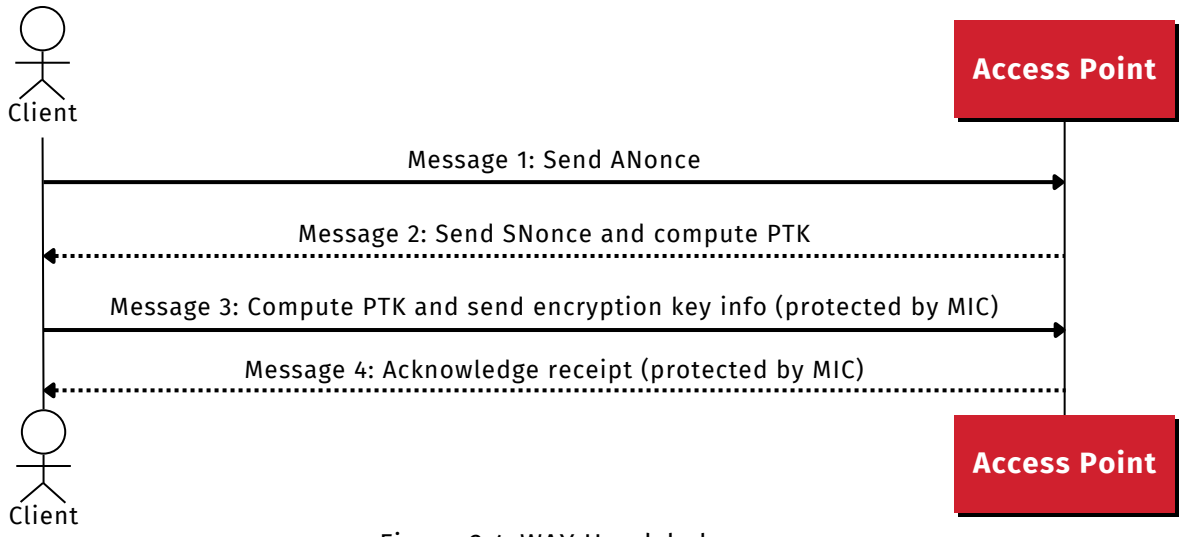

Figure 2 4-WAY Handshake

PTK = KCK + KEK + TK
MIC = HMAC SHA-1 (KCK)

Key Breakdown:
EAP over LAN (EAPOL) Key Confirmation Key (KCK). Performs proof of procession of PMK access-control function. This in turn facilitates the integrity and data origin authenticity between the STA and AP.

EAPOL Key Encryption Key (EAPOL-KEK). Protects the confidentiality of keys during initial RSN association.

Temporal Key (TK). Used to encrypt actual user traffic that is unicast between the STA and the AP.

3.2 Group Handshake

A Group Handshake is necessary when the STA is participating in multicast or broadcast traffic. After the Group Handshake is completed the AP and client (STA) can start Protected data exchange.

Phase 4 Protected Data Exchange

Protected Data Exchange is the fourth phase of RSN. By this stage, both the AP and STA have authenticated each other, and generated keys for encryption. The data can now be encrypted using the confidentiality algorithm chosen.

Vulnerabilities

PMKID Hash Dictionary Attack

While researching methods to break WPA3, it was discovered that a dictionary attack on WPA2 is possible without the need for capturing the 4-WAY handshake. This attack is performed on the RSN IE of the EAPOL frame, which is received right before the 4-way handshake. Once the packet is captured, analysis tools like Wireshark can be used to find the PMKID, which is calculated using the following formula:

$$PMKID = HMAC\text{-}SHA1\text{-}128(PMK, \text{"PMK Name"} \mid MAC\_AP \mid MAC\_STA)$$

PMK Name is a fixed non-changing string. The other two fields are the MAC addresses of the AP and STA. With this information available, the adversary can compute PMK using candidate PSK computed from the Word list of phrases and cross-check if the hash matches the one captured in PMKID. This attack can be mitigated using a strong password.

4-Way Handshake Phase Attacks

KRACK is a combination of attacks targeted at a 4-way handshake. It exploits the specific implementation flaw where the adversary lets the first three messages of the handshake complete normally. However, by acquiring the Man-in-the-Middle (MITM) position, it blocks message 4 from the client to AP, resulting in key reinstallation (hence the name KRACK or Key Reinstallation Attack). Now, to understand how that leads to decryption, we need to take a step back and examine how keystreams are used in the encryption process.

Though AES, the encryption algorithm, is not attacked, it's the next step in the algorithm that is vulnerable. The first message from the client to the AP is simply the plaintext data XORed with the keystream (which is the PTK scrambled with some other parameters). This construct leads to the vulnerability.

To further analyze, plaintext P is XORed with the keystream K to generate the encrypted result E:

$$E = P \oplus KS$$

If that's the case, and somehow an adversary is able to capture two encrypted packets, then this information can lead to decryption because the keystreams are the same. XORing the two encrypted texts will cancel out the keystreams and leave the two plaintexts.

Given:

$$E' = P' \oplus KS'$$
$$E'' = P'' \oplus KS''$$

Then:

$$KS = KS' = KS''$$
$$E' \oplus E'' = P' \oplus P''$$

If the adversaries can guess or know P', they can decrypt P''. While this is a bit of mathematical background, it should help you understand how a specific series of events makes this attack possible.

Key Reinstallation Process

Here's how key reinstallation happens:

- The adversary establishes a MITM position between the client and the AP.
- It lets the first three messages continue as usual
- It blocks message 4 of the handshake to the AP

This leads to an interesting scenario: from the client's perspective, it has already derived and installed the Session Key. So it will send the encrypted message to the AP, but if the AP has not completed the handshake, it will try to recover from this situation by retransmitting message 3 of the handshake as per the standard.

- The client receives message 3 from the AP with the replay counter value of r+2.
- The client replies to AP with the encrypted message 4 using a Packet Number of 1.
- The client then reinstalls the key and the next data frame will have the same packet number.

The adversary now has original message 1 of the handshake, which was plaintext, and the retransmitted message 4 (only the replay value is changed; the rest of the parameters are almost identical.) XORing these two will reveal the keystream KS, which corresponds to packet number 1. This keystream can be used to decrypt the first data packet, resulting in the retrieval of plaintext.

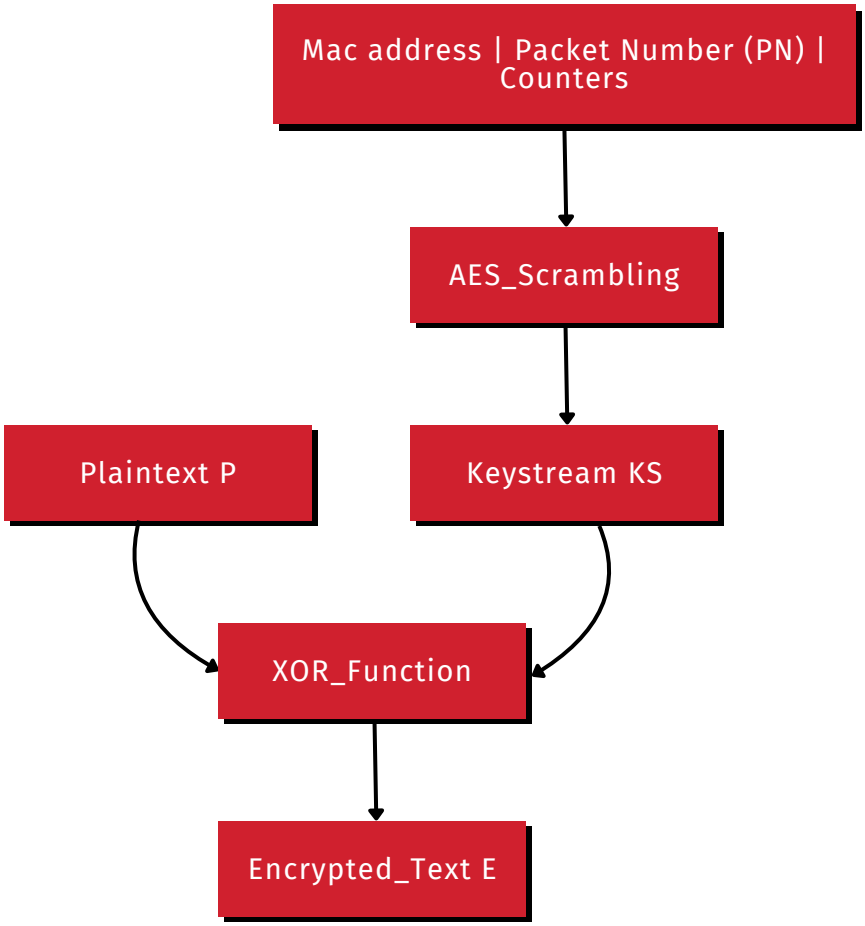

Figure 3 KRACK Steps

Mitigations

To mitigate the attacks there are several industry-recommended solutions. Each of them will be individually evaluated based on the size of the network and the organizational needs.

IDS/IPS

For a small to medium-sized organization with strict security requirements, an open-source IDS (intrusion detection system) and IPS (intrusion prevention system) can be a powerful tool to detect suspicious activity on the air interface using Snort and Raspberry Pi.

- Deploy Snort on Raspberry PI and configure it to monitor the required WLAN interface.
- Develop custom Snort rules to detect KRACK attack patterns, such as multiple retransmissions of 4-WAY Handshakes in specific time intervals.

This will have scalability issues.

Update Firmware

Updating Firmware looks like the easiest of all, but it depends on what your wireless environment looks like, what sort of client's devices you have, their OS, etc. Although there is a Python Script available online, work can be done to add a graphical user interface for widespread adoption, enabling enterprises to validate their devices against potential upgrades.

Countermeasure

As WPA2 has been widely adopted, it would be fair to assume that some IoT devices, mainly in hospitals and other critical infrastructure would never get a patch. In that case, APs can prevent the attacks on the clients by not retransmitting the later frames of the 4-WAY handshake. However, the impact on the resilience and coverage of the wireless network will need to be assessed, and alternative means might be required to make the solution work.

WPA3

WPA3 is the latest security standard introduced to address the concerns related to WPA2 and it brings significant improvements in terms of encryption, authentication, and privacy. Some of the enhancements rolled out are as follows:

- **Simultaneous Authentication of Equals (SAE)**: Provides resistance against offline dictionary attacks.
- **Operating Channel Validation (OCV)**: Protects against Man-in-the-Middle (MitM) attacks like KRACK.
- **Protected Management Frames (PMF)**: Mandatory protection for management frames.
- **Opportunistic Wireless Encryption (OWE)**: While not a direct component of WPA3, an often enabled standards-based solution that enables wireless devices to establish encrypted connections on public hotspots without requiring a passphrase.
- **192-bit Security Suite**: Offers stronger cryptographic algorithms for environments with stringent security requirements.

WPA3-Personal supports two modes of operations:

- WPA3 Mode: Uses SAE protection and implements the use of Protected Management Frames (PMF). This mode requires wireless clients to support WPA3 obligatorily.
- WPA3 Transition Mode: Provides backward capability for WPA2 clients to co-exist on the same SSID if the clients do not support WPA3-SAE. In this mode, AP advertises PMF as an optional legacy device that connects without it while modern devices connect using SAE and PMF.

Simultaneous Authentication of Equals

SAE incorporates Dragonfly (RFC7664) which is Password Authentication Key Protocol (PAKE) and provides peer-to-peer communication and uses Elliptic Curve Cryptography. SAE provides forward secrecy and mutual authentication.

- Commit Phase: Client and AP exchange cryptographic messages to generate a common shared secret
- Confirm Phase: Both Client and AP confirm they have derived the same secret and are in turn possession of the same password.

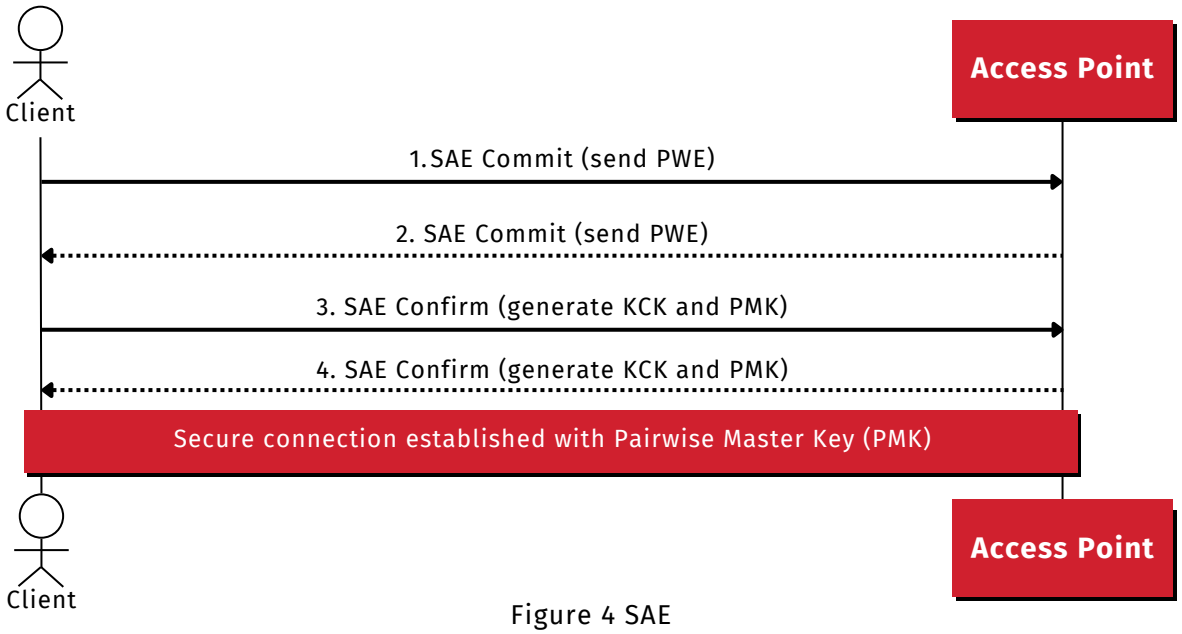

Figure 4 SAE

Vulnerabilities

Downgrade and Dictionary Attack

In transition mode, the AP accepts both WPA2-PSK and WPA3-SAE client connections. WPA3 provides forward secrecy by providing authenticated RSNE in the WPA2 4-way handshake allowing the client to detect if the beacons are forged. Although protection from downgrade attacks is provided by the WPA2 handshake only a single authenticated handshake is required to be captured. This enables an adversary to perform a dictionary attack by forging the first message of the handshake, as it is not authenticated.

Some mitigation strategies include:

- After associating using SAE, the client should store the networks supporting SAE, preventing connections using a weaker handshake.
- Deploying separate WPA2 and WPA3 networks can also help remediate this vulnerability.

Denial of Service Attack

Dragonfly's high overhead can be abused by an adversary by spoofing commit frames to perform a Denial-of-Service attack. To defend against it, an anti-clogging mechanism was added to SAE. In this defense, the client must present a cookie sent by the AP that helps protect resources before committing to expensive operations.

An adversary can capture and replay cookies to perform a DoS attack. The attacker can spoof MAC addresses directed towards the AP, which, upon suspicion of an attack, sends a secret cookie requesting the client's authenticity. The attacker reflects this to the AP, forcing it to perform expensive cryptographic operations.

Mitigation options include rate-limiting to limit the number of commits an AP will perform in a limited time span, or enhancing the validation mechanism for cookies.

Beacon Protection

WPA3 incorporates beacon protection features to protect against active attacks in which beacon information elements can be forged to alter the client's power consumption, data rates, and channel switch executions. The addition of Message Integrity Check and Beacon Integrity Key to Beacon frames is performed during client associations.

Operating Channel Validation

Operating Channel Information (OCI) is introduced to provide resiliency against KRACK attacks. The OCV feature introduces OCI to the 4-WAY handshake. If the AP finds that the information does not match with the received channel, it aborts the connection and the same procedure is performed by the client. Attackers can no longer gain a multi-channel MITM position to block or replay message 3 of the handshake.

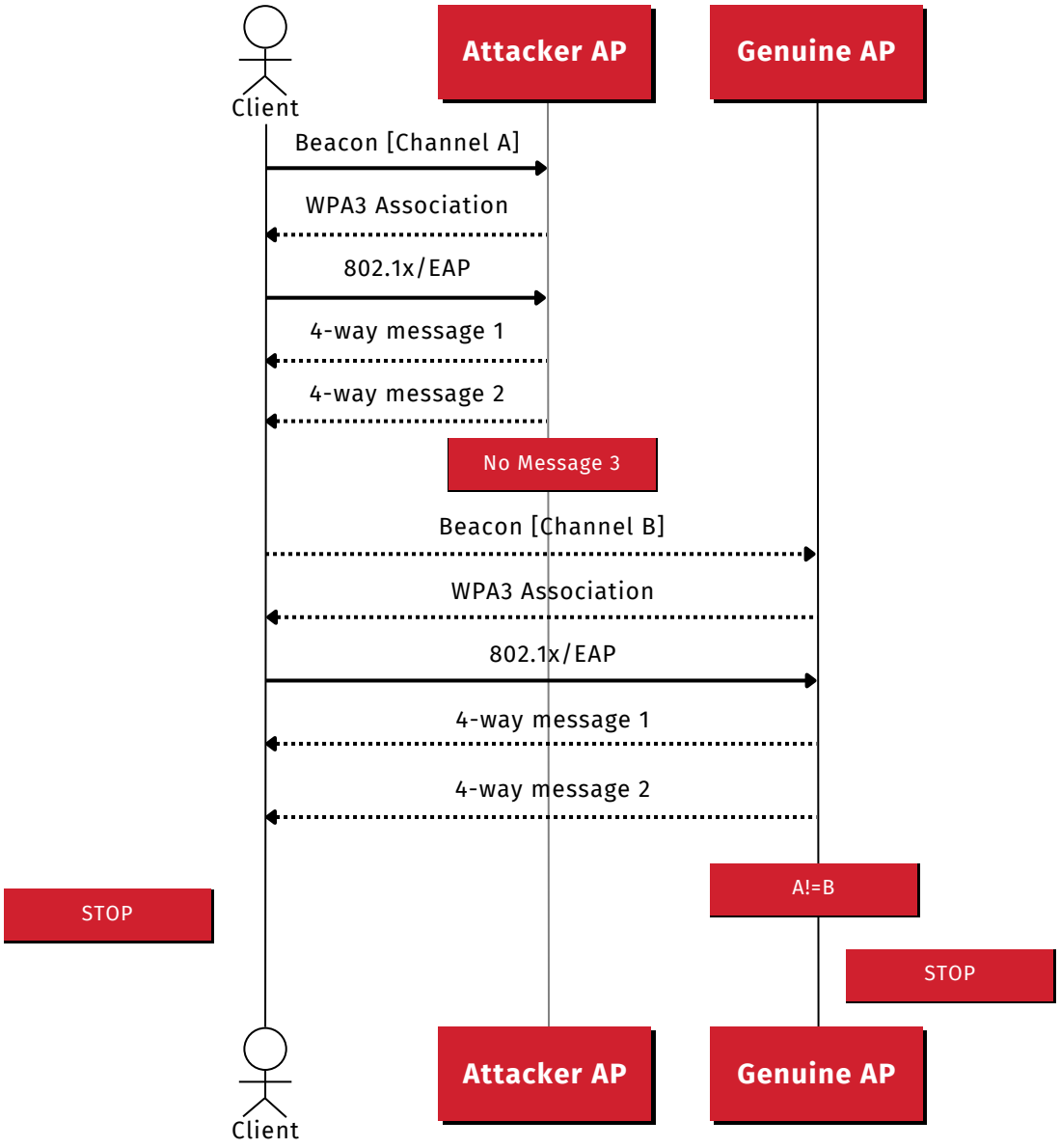

Figure 5 OCV

Opportunistic Wireless Encryption

OWE provides encryption for data exchanged within open networks to make them resilient to eavesdropping and interception. With OWE, encrypted data between the client and AP can now be exchanged without the need for a shared password. Some of the key features provided by OWE are:

- Automatic encryption for open networks
- No user intervention required
- Mitigation against eavesdropping

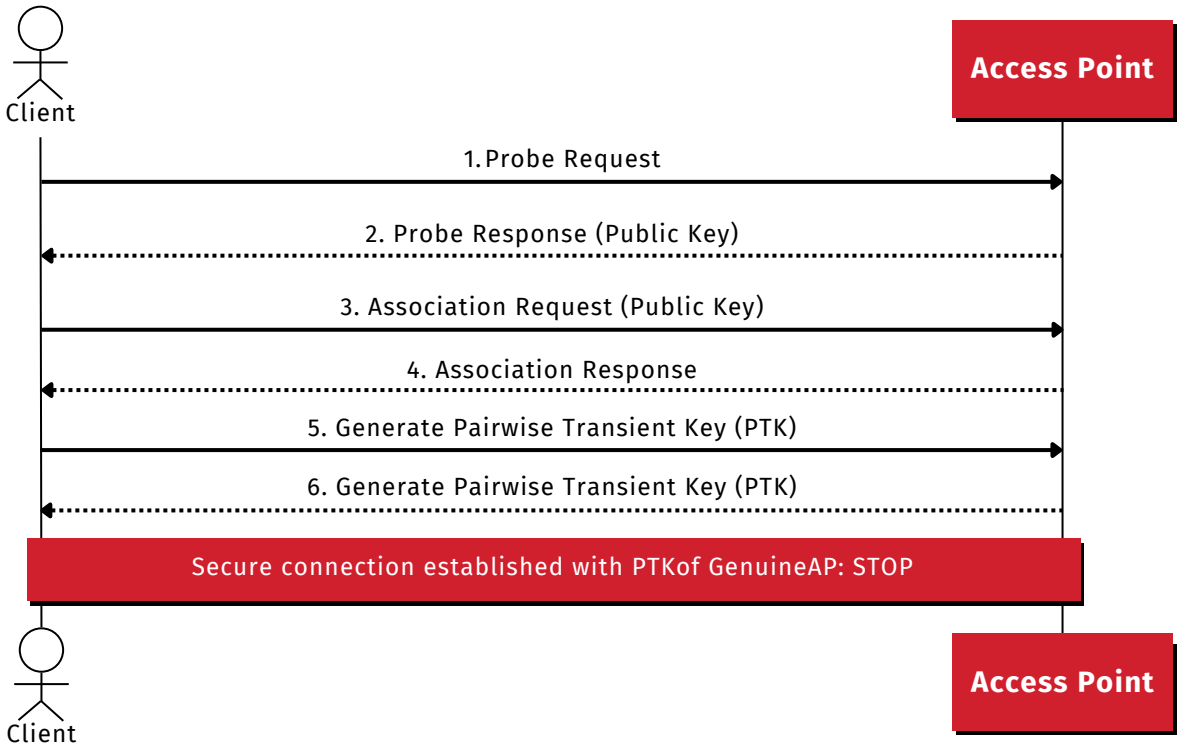

Figure 6 OWE

SUMMARY

In conclusion, WPA3, while having some vulnerabilities itself, is far superior to WPA2 and the discovered vulnerabilities have been addressed in the vast majority of systems that implement it. While many environments still require the use of WPA2 to support legacy client devices, options are available to monitor and enforce security in those networks. With WPA3 and OWE required in the 6 GHz band, the future will see significantly increased availability and use of both as the clients and APs implementing 6 GHz radios will have the same logic to use for all supported bands. This reality will usher in a more secure era of WLAN networking.

References

https://papers.mathyvanhoef.com/ccs2017.pdf
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-97.pdf
https://doi.org/10.3390/electronics7110284

Melissa Rowland | Global Account Executive (Sales) **melissa@cwnp.com** **cwnp.com**