Exploring Wi-Fi Security Protocols - WPA2 vs WPA3

Prepared By:

Arunima Negi	(30281210)
Huma Naiman	(30303242)
Karanveer Singh	(30282286)
Pradip Ghimire	(30303867)

Introduction

Wireless communication has become an essential part of our daily lives. We now have the luxury of accessing the internet from our homes, offices, schools, and various other public locations with the use of Wi-Fi. Unfortunately, Wi-Fi isn't the same as a cable network and transmits data via radio waves, so anyone within the range can connect themselves to the network or even intercept or manipulate traffic. Because of this, wireless networks face serious security risks. Attackers may intercept private data, manipulate traffic, or take over devices if the network is not well protected.

To reduce these risks, security protocols were created. These protocols are rules which explicitly tell how the transmitted data must be encrypted, the procedure of user authentication, and so on and so forth. The Wi-Fi Protected Access (WPA) family of protocols represents the most widely adopted security standards for wireless networks [1].

This document discusses the evolution of Wi-Fi security protocols with an emphasis on WPA2 and WPA3. Analysis of their architecture, encryption mechanisms, key exchange methods, and vulnerabilities was provided. By critically analyzing the benefits and drawbacks of WPA2 and WPA3, the report emphasizes the importance of continuous improvement of wireless security systems to keep up with the evolution of threats under current electronic conditions.

Evolution of Wi-Fi Security Protocols

The need for secure wireless communication has driven the development of several protocols over the past two decades. Each generation aimed to fix weaknesses in its predecessor:

WEP (Wired Equivalent Privacy)

WEP was introduced in 1997 as part of IEEE 802.11 standard. The engineers developed it to give wireless networks the same degree of privacy as wired networks. It uses RC4 stream cipher Encryption Algorithm to encrypt the WEP data. Prior implementations of the key had a 40-bit key (typically referenced as WEP-40) with a 24-bit Initialization Vector (IV), giving 64 bits altogether. [2] Later versions strengthened the secret key to 104 bits (more commonly referred to as WEP-128, though actually 104 + 24 bits) to boost security. WEP use two types of authentications i.e. Open system Authentication (OSA) and shared key Authentication (SKA). Open System Authentication means client initiates connection; the access point approves/denies based on SSID matching, without requiring any encryption credentials [2]. In SKA a four-step challenge-response process is used where the access point sends a challenge to the client, the client encrypts it using the shared WEP key, and the access point verifies the response. But this method is also weak in practice.

Vulnerabilities and weaknesses: WEP uses weak RC4 encryption with short 24-bit IVs, poor key management, and no authentication, allowing attackers to easily capture packets and crack network keys.

WPA (Wi-Fi Protected Access)

WPA was introduced in 2003 by the Wi-Fi Alliance as a solution to the vulnerabilities of WEP to give superior security without the requirement of new hardware. Existing devices that supported WEP could be upgraded its firmware to support WPA. The WPA applies the TKIP (Temporal Key Integrity Protocol) protocol, also founded on the RC4 stream cipher (as in the case of the WEP), but with additional wrapping in order to minimize the known weaknesses of the WEP [1]. In contrast to the static key usage of WEP, the TKIP will change or "mix" the key with each packet, utilizing a per-packet key mixing algorithm. This reduces the ability of the intruder to reuse the intercepted packets to derive the key. TKIP mixes the secret "base" key with the IV and the rest of the parameters to generate a new per-packet key [3]. This "key mixing" acts to hide vulnerabilities that are known with naive key re-use. It used Pre-Shared Key (PSK) i.e. The passphrase or password that all authorized clients as well as the access point are known to. This is the home or small-office default installation. For the businesses it uses 802.1X Enterprise Mode: Provides authentication to the authentication server externally (such as RADIUS), which uniquely authenticates the credentials of each client. Instead of the insufficient integrity check (CRC-32) of WEP, the WPA features a MIC (occasionally referred to as "Michael"), a keyed hash that should ensure that no attacker can alter the packets [4]. The MIC operates to filter out efforts to alter or inject false frames.

Vulnerabilities & Weaknesses: WPA's TKIP encryption and MIC are outdated, making it vulnerable to replay and dictionary attacks, downgrade exploits, and weak password guessing in pre-shared key networks.

WPA2 (Wi-Fi Protected Access II)

WPA2 is the Wi-Fi Alliance certification for the complete use of the IEEE 802.11i extension, standardized in 2004. WPA2 replaces weaker standards of WEP. WPA2 needs AES (Advanced Encryption Standard) with CCMP (Counter Mode with CBC-MAC) to be used for confidentiality as well as integrity [1]. So, AES-CCMP assures the data to be both encrypted as well as secure from tamper attacks or replay attacks. Like WPA, WPA2 also has personal and enterprise modes of authentication. WPA2 added the 4-Way Handshake to safely generate session-independent encryption keys (the "Pairwise Transient Key" or PTK) and to mutually verify knowledge of the master key without ever transmitting it in the clear. The handshake also guarantees freshness (nonces) and maintains synchronized counters. Since 2006, WPA2 (i.e., devices supporting AES-CCMP / 802.11i) have been mandatory for Wi-Fi certification [3].

Vulnerabilities & Weaknesses: WPA2 is vulnerable to KRACK (Key Reinstallation Attack), weak pre-shared passwords, lack of forward secrecy, and attacks on unprotected public networks using handshake exploitation.

WPA3 (Wi-Fi Protected Access III)

WPA3 is the latest WI-FI security standards introduced by the Wi-Fi Alliance in 2018. It was built upon WPA2 by enhancing encryption, authentication, and privacy. WPA3 uses AES-CCMP encryption, which is similar to WPA2, but replaces the Pre-Shared Key (PSK) method with Simultaneous Authentication of Equals (SAE) in personal mode. SAE is a password-authenticated key exchange protocol that provides better resistance to offline dictionary attacks [1].
In WPA3 Enterprise mode, it supports a stronger 192-bit encryption suite, with strong security that is ideal for enterprise networks. WPA3 provides forward secrecy since new session keys are generated during every connection. This implies that even if the future password is hacked, old communications will be secure. Opportunistic Wireless Encryption (OWE) offers encryption to open (password-less) Wi-Fi networks, such as airport or cafe networks [5]. OWE encrypts the traffic without the need for user authentication to prevent eavesdropping as well as man-in-the-middle attacks. Also, Protected Management Frames (PMF) strengthen security by securing management frames, which are utilized during device disassociation and association tasks. This aspect preserves the vulnerability to deauthentication attacks, among others that exploit management frames.

Vulnerabilities & Weaknesses: WPA3 faces risks from Dragonblood side-channel attacks, downgrade exploits in transition mode, and implementation of flaws that can expose passwords or weaken encryption if not properly patched.

Security Protocol Standards in Wi-Fi

Wi-Fi security protocols are based on the IEEE 802.11 family of standards, which define the technical specifications for wireless local area networks (WLANs). The key security standards include:

1. **IEEE 802.11i:**
   The IEEE 802.11i amendment was developed to correct significant weaknesses in previous Wi-Fi standards such as WEP (Wired Equivalent Privacy) and the then prevalent TKIP (Temporal Key Integrity Protocol). The new standard brought with its AES-CCMP (Advanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), the new default encryption standard that replaced outdated, easily exploitable algorithms. 802.11i essentially underpinned the

development of WPA2, the international standard of Wi-Fi security beginning in 2004. This amendment standardized strong encryption and authentication procedures, guaranteeing enhanced data security and resistance to prevalent attacks [6].

2. **802.1X:**

   IEEE 802.1X is a form of authentication framework that includes the port-based network access control found commonly in enterprise Wi-Fi networks. The framework supports both the use of WPA2-Enterprise as well as WPA3-Enterprise modes, with the use of the external authentication server such as RADIUS (Remote Authentication Dial-In User Service) to verify the user's credentials. Diverging from home networks that use one shared password, 802.1X enables organizations to use the individual user credentials, enhancing accountability as well as security [7]. The framework supports different EAP (Extensible Authentication Protocol) methods, supporting integration with smart cards, digital certificates, or systems of multi-factor authentication.

3. **AES (Advanced Encryption Standard):**

   AES is a secure block cipher encryption protocol that has been made a worldwide standard through the approval of the U.S. National Institute of Standards and Technology (NIST). AES replaces outdated encryption protocols such as DES and is prevalent in industries as well as Wi-Fi security. AES encrypts data in blocks of a fixed size with the help of 128, 192, or 256-bit secret keys. AES in Wi-Fi networks ensures that the information exchanged between connected devices and the router remains incomprehensible to eavesdroppers. The version incorporated within WPA2 as well as WPA3 (AES-CCMP) also preserves the integrity of the message to avoid the tampering or injecting of data packets with the help of the attackers [8].

4. **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol):**

   CCMP is the Wi-Fi protocol that encrypts AES. CCMP uses two cryptographic schemes:

   - Counter Mode (CTR): Manages encryption by making AES a stream cipher that encrypts information quickly.
   - Cipher Block Chaining Message Authentication Code (CBC-MAC): Provides data integrity as well as authenticity verification.

   These together prevent replay attacks, whereby the intruders attempt to resend data packets that are intercepted and ensure that the sent messages are unchanged [8]. CCMP is designed to be a successor of TKIP that offers significantly increased security as well as stability.

5. **SAE (Simultaneous Authentication of Equals):**

   SAE is a new authentication protocol that was added with WPA3 in order to supersede the old 4-Way Handshake found in WPA2. It's founded on the cryptographic method known as the Dragonfly Key Exchange, enabling two devices to safely mutually authenticate each other without revealing passwords, even if communication can be intercepted [9]. SAE offers effective resistance to dictionary attacks as well as brute-force attacks, as attackers can't readily try passwords off-line. SAE also adds forward secrecy, indicating that if the Wi-Fi password is hacked later, previous sessions will be secure. This makes networks that use WPA3 significantly harder compared to modern attacks as well as password-cracking attacks.

WPA2

WPA2 is the implementation of IEEE 802.11i-2004, which upgraded Wi-Fi security by specifying enhancements in authentication, confidentiality, and integrity protection for data transmitted over wireless networks. Under 802.11i, a wireless network that supports the full set of security enhancements is called a **Robust Security Network** **(RSN)**. An RSN requires stations (clients) and access points (APs) to perform defined authentication protocols and secure key exchange before permitting data traffic. WEP is deprecated under 802.11i; WPA (with TKIP) was an intermediate step, but AES-based CCMP is mandatory for full RSN compliance. [11]

RSN under WPA2 defines two key hierarchies: the ***pairwise key hierarchy*** (which handles unicast links between a station and AP), and the ***group key hierarchy*** (which is used for multicast/broadcast traffic). The latter is needed since multicast or broadcast frames go to multiple stations, so a shared group key (GTK) is distributed in a secure manner. [11]

Key Derivation & the 4-Way Handshake

PMK to PTK Derivation

The Pairwise Master Key (PMK) can come from either a Pre-Shared Key (PSK) in personal mode or from an EAP/802.1X authentication process in enterprise mode. [12]

To derive the Pairwise Transient Key (PTK), the handshake uses several inputs:

1. PMK
2. ANonce (random nonce generated by the Access Point)
3. SNonce (random nonce generated by the Station(STA)/client)
4. MAC address of AP
5. MAC address of STA/client

A pseudo-random function (PRF) processes these inputs to produce PTK. A PTK is then split into multiple sub-keys: **KCK** (Key Confirmation Key, used for message integrity), **KEK** (Key Encryption Key, used for encrypting the GTK and some key data), and **TK** (Temporal Key, used for actual data frame encryption). [12]

Steps of the 4-Way Handshake:

Here are the handshake messages, with detail:

Message	**From → To**	**Content**	**Purpose**
Msg 1	AP → STA	ANonce + RSN parameters	AP starts and provides random challenge (ANonce)
Msg 2	STA → AP	SNonce + MIC (derived using KCK)	STA shows SNonce, computes preliminary PTK, proves knowledge of PMK
Msg 3	AP → STA	GTK encrypted under KEK + MIC	AP sends group key, ensures STA can receive group/broadcast traffic, installs keys
Msg 4	STA → AP	ACK + MIC	Confirmation from STA that the keys are installed and working

- Fresh nonces (ANonce & SNonce) ensure that each handshake produces a fresh PTK.
- The protocol mandates that PMK itself is never transmitted over the air. All required shared secretness is derived. [12]

Step-by-step breakdown:

Message 1: AP to STA (ANonce + RSN Parameters)

The Access point initiates the handshake by sending a random number, called the ANonce (AP Nonce), along with RSN (Robust Security Network) parameters such as supported ciphers and key management methods. This message serves as a challenge and signals the start of key derivation. The ANonce is unique for each session to ensure fresh encryption keys.

Message 2: STA to AP (SNonce + MIC)

Upon receiving the ANonce, the Client (denoted as STA) generates its own random number, the SNonce (Station Nonce). The client uses the ANonce, SNonce, PMK, and the MAC addresses of both devices to compute the Pairwise Transient Key (PTK). It then sends the SNonce along with a Message Integrity Code (MIC), which is derived using the Key Confirmation Key (KCK) from the PTK. This proves the client possesses the PMK without transmitting it.

Message 3: AP to STA (GTK encrypted + MIC)

The AP receives the SNonce and now both sides can compute the PTK. The AP encrypts the Group Temporal Key (GTK) using the Key Encryption Key (KEK) from the PTK and sends it to the client along with a MIC. Installing the GTK allows the client to decrypt broadcast and multicast traffic. The AP also confirms to itself that the client can now participate securely.

Message 4: STA to AP (ACK + MIC)

Finally, the client acknowledges that both PTK and GTK have been successfully installed by sending an ACK along with a MIC. This completes the handshake. From this point on, both the AP and the client use the PTK for unicast encryption and the GTK for multicast/broadcast traffic. [12]

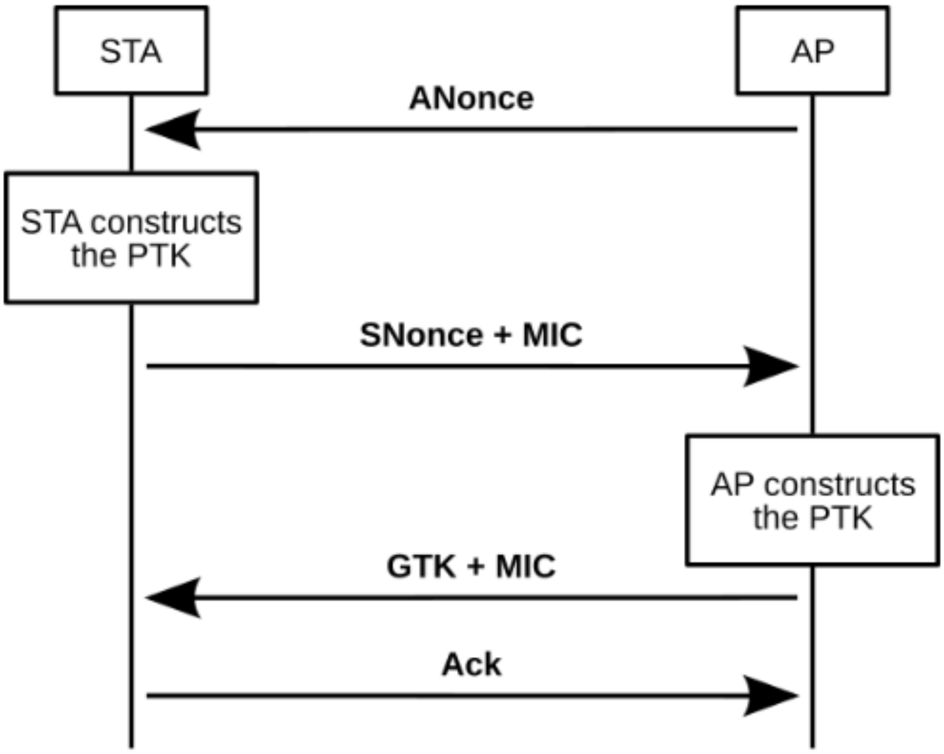


Figure 1: The WPA2 4-Way Handshake between client and access point for Mutual authentication and key exchange process to establish a secure encrypted session. [11]

Encryption: AES-CCMP Details

CCMP (Counter Mode with CBC-MAC Protocol) combines AES in Counter Mode (CTR) for confidentiality with CBC-MAC for integrity and authentication. It protects the data payload of MAC Protocol Data Units (MPDUs) and certain header fields, ensuring data cannot be read or tampered with undetected. Older protocols like WEP or WPA/TKIP do not offer equivalent integrity protection, and AES-CCMP uses a long nonce to prevent IV reuse [13], [11].

Trade-Offs, PSK vs Enterprise & Additional Weaknesses

PSK (Pre-Shared Key) mode: This mode is easy to set up because you just need a shared password. However, if the password is weak, attackers can guess it using offline attacks. Also, every device on the network uses the same key. This means that if one device is compromised, the security of all devices is affected [15], [14].

Enterprise mode (802.1X/EAP): This mode is more complex because it requires an authentication server and certificates for each user or device. It allows for features like revoking access for a user and ensures both the user and the network verify each other. Because of this, it is generally more secure than PSK. But even Enterprise mode can still be vulnerable if the handshake allows keys to be reused or reinstalled incorrectly [15], [14].

Additional weaknesses:

Fallback and mixed modes: Some networks are set up to allow older security methods, like TKIP, for compatibility. Attackers can force the network to use these older, weaker methods to break the security [15].

Frame size leakage: Even with strong encryption, some information, like the size of packets and the timing of messages, can be observed. This can give attackers clues to launch side-channel attacks [11].

Lack of forward secrecy: If an attacker captures the main key (PMK), they could decrypt past communications if the keys are reused or if the random numbers (nonces) are predictable [11].

Improvements and What WPA2 Does Correctly

Using AES-CCMP in WPA2 fixes many problems found in older Wi-Fi security like WEP and TKIP, such as weak encryption, repeated initialization vectors (IVs), and poor integrity checks. WPA2's handshake uses new random numbers (nonces) and verifies both the client and the network, which makes it harder for attackers to eavesdrop. For attacks like KRACK, applying the proper updates prevents keys from being reused and stops counters from being reset, keeping the connection safe [11], [14].

Real World Attack: KRACK (Key Reinstallation Attack) on WPA2

The KRACK (Key Reinstallation Attack) vulnerability in WPA2 was first discovered by Belgian researchers Mathy Vanhoef and Frank Piessens from the University of Leuven in 2016. They found that the flaw affected the core of the WPA2 protocol itself, rather than just individual device implementations [16]. Details of the attack were publicly revealed in October 2017 after coordinating disclosure to vendors and the US-CERT security organization.

The research group presented the technical details at the ACM Conference on Computer and Communications Security in November 2017. After disclosure, urgent global efforts were made to patch affected systems, but many devices—especially older ones—remained vulnerable for an extended period. The vulnerability impacted nearly all devices using WPA2, including Windows, Linux, Android, iOS, and macOS.[16]

KRACK (Key Reinstallation Attack) targets a critical vulnerability in the WPA2 protocol's four-way handshake, which is used by devices and access points to securely establish encryption keys for Wi-Fi communication.[16]

KRACK can affect both Personal and Enterprise modes. In some cases, a vulnerable device may even set its encryption key to all zeros, making it very easy for attackers to decrypt the data.

WPA2 Four-Way Handshake Key Terms

- PMK (Pairwise Master Key): The main shared key between client and AP, derived from the Wi-Fi password or authentication handshake.
- PTK (Pairwise Transient Key): Key for encrypting unicast (one-to-one) traffic between each client and access point, generated uniquely for every session.
    - PTK is derived from:
        - PMK
        - ANonce (AP's random number)
        - SNonce (client's random number)
        - both MAC addresses (AP and client)
- GTK (Group Temporal Key): Used for encrypting multicast and broadcast traffic sent from the AP to multiple clients.
- Nonce: A "number used once." ANonce comes from AP, SNonce from client. Both are random values, ensuring that every encryption session is unique.
- MIC (Message Integrity Code): Ensures handshake messages haven't been tampered with.
- Replay Counter: Value to detect and prevent replay attacks using old handshake messages.[16]

Step-by-step Handshake & Attack (see diagram)

When a client device connects to a WPA2-secured Wi-Fi network, it performs a four-step handshake with the access point:
1. The access point sends a nonce (a random number) to the client.
2. The client uses this nonce and its own nonce to derive a fresh encryption key.
3. The client sends confirmation back to the access point that it installed this key.
4. The access point acknowledges this confirmation.
This handshake ensures that both parties have the same fresh encryption key to encrypt subsequent data securely.

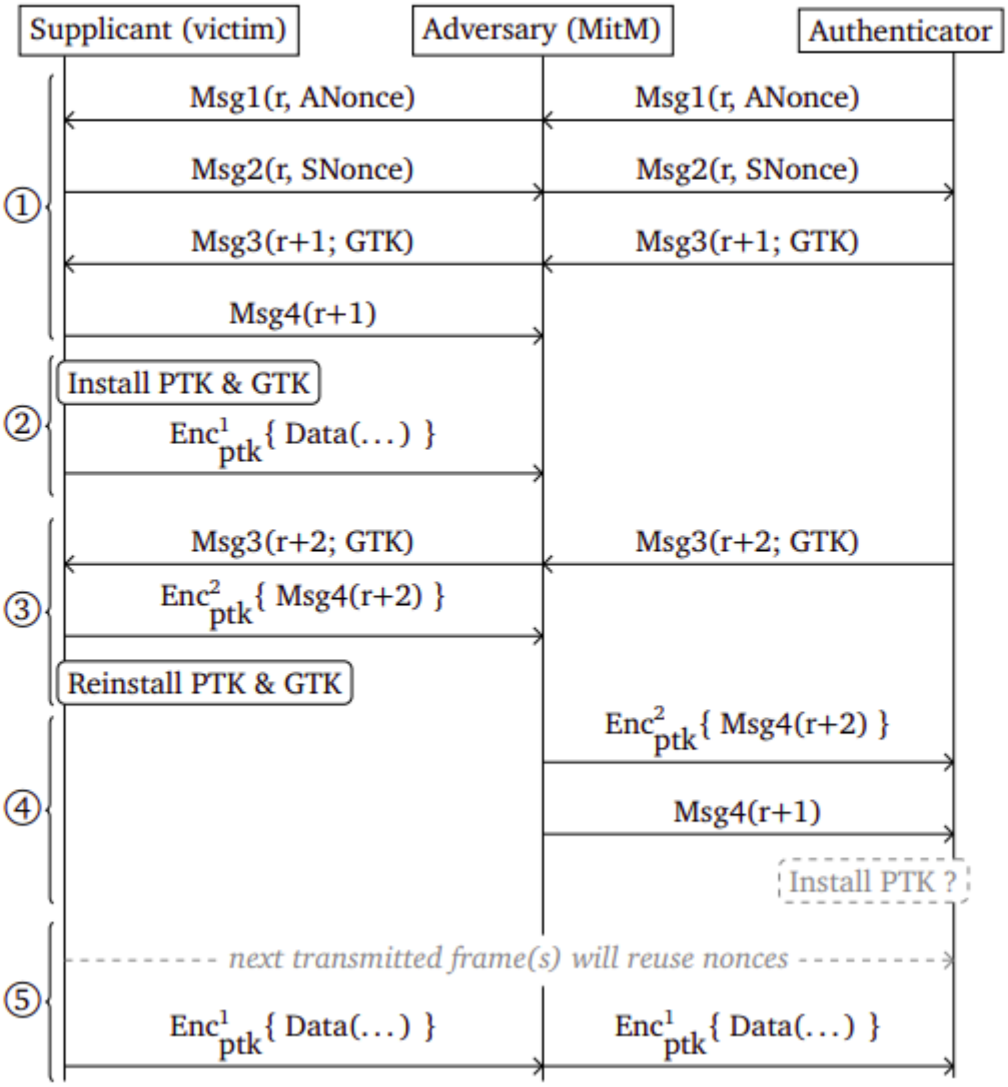


Figure 2: Man-in-the-middle adversary can exploit nonce and key reinstallation vulnerabilities during Wi-Fi authentication between a supplicant, adversary, and authenticator. [16]

KRACK's Exploitation Technique

KRACK exploits the fact that the third handshake message can be retransmitted multiple times by the access point if it doesn't receive an acknowledgment from the client. This retransmission behavior is normal to handle wireless packet loss.

An attacker in wireless range can capture and replay these third handshake messages to the client multiple times. Each time the client receives this message, it reinstalls the same encryption key instead of recognizing it as a retransmission. Upon reinstalling the key, the client resets important security parameters:

- The nonce (the incremental transmit packet number) is reset to its initial value.
- The replay counter used to detect packet replay attacks is also reset.

Resetting the Nonce

Encryption protocols like AES-CCMP rely on the nonce being unique for every encrypted packet to maintain confidentiality and integrity. When the nonce is reset and reused:

- Packets encrypted with the same key and nonce combination become vulnerable to replay and decryption attacks.

- Attackers can decrypt, replay, or forge Wi-Fi packets, breaking the presumed confidentiality of the wireless communication.[16]

Exploitability

KRACK exploits a vulnerability in the four-way handshake process of WPA2, specifically the third message of the handshake. This handshake is how the client and access point confirm the Wi-Fi password and establish encryption keys.[16] This handshake is only needed when initially connecting, but the third message can be retransmitted multiple times to speed up reconnects. KRACK tricks the victim's device into reinstalling an already-in-use encryption key by replaying this message repeatedly. This causes nonce and replay counters to reset, breaking encryption security by creating nonce reuse, allowing attackers to decrypt, replay, or inject Wi-Fi packets.[16]

Range of attack

KRACK attacks require the attacker to be in close wireless proximity to the victim, typically within the same Wi-Fi signal range, usually tens to a few hundred meters. This is because the attacker needs to intercept and manipulate Wi-Fi handshake messages exchanged between the client device and the access point.

Attack Surfaces

- The handshake protocol between client devices and Wi-Fi access points.
- Client devices' Wi-Fi software, implementations with flaws in key management like wpa_supplicant used in Linux and Android.
- Networks using WPA2 personal and enterprise modes, including those using AES or TKIP encryption.
- Any device connecting to vulnerable access points within radio range.[16]

Damage Potential

- The vulnerability affected nearly all WPA2-enabled devices worldwide, including major operating systems like Windows, macOS, iOS, Android, and Linux.
- About half of Android devices were severely vulnerable due to an additional bug allowing installation of an all-zero encryption key, effectively nullifying security.
- Attackers could decrypt sensitive data such as passwords, emails, credit card numbers, and hijack session connections.
- The attack allows injection of malicious data packets, potentially spreading malware or ransomware.
- The exposure compromised billions of devices globally until patches were applied.

Impact on Different Devices

KRACK affects nearly all WPA2 implementations because the vulnerability stems from the WPA2 protocol design rather than individual device flaws.[16] However, some devices are more severely impacted:

- Linux and Android devices using the wpa_supplicant implementation can be tricked into reinstalling an all-zero encryption key, effectively nullifying security.
- Other devices may not install an all-zero key but remain vulnerable to partial packet decryption and replay.

WPA3

WPA3 is the Wi-Fi Alliance's successor to WPA2 that changes the default client authentication model from a static PSK (pre-shared key) to a password-authenticated key exchange based on the Dragonfly construction. This design goal is to provide mutual authentication, protection against offline dictionary attacks, and forward secrecy for personal wi-fi networks, while also improving enterprise-grade options for higher security suites. [17]

When you connect to Wi-Fi, your device and router perform a 'handshake' to prove you know the password. In WPA2, attackers could record this handshake and take it home to crack your password using powerful computers without ever touching your network again. This is a passive attack impossible to detect.
WPA3 changes how the handshake works. Instead of something that can be recorded and cracked offline, WPA3 forces attackers to test each password guess against your actual network in real time. This makes attacks -

- 1000x slower (seconds per attempt vs millions per second)
- Easily detectable (you see the attack happening)
- Easily blockable (you can stop the attacker)

What is new in WPA3

As the name suggests, WPA3 is the successor of WPA2. WPA3 is a certification program, and it supports four major features of which only one is mandatory which is the new dragonfly handshake and use of Protected Management Frames (PMF). Those four features are the following -

- A new handshake called dragonfly (also called Simultaneous Authentication of Equals) that is resistant against dictionary attacks and provides forward secrecy. Makes use of Zero knowledge proofs.
- A straightforward method to securely add devices to a network. Referred to as Wi-Fi CERTIFIED Easy Connect program.
- Protective mechanisms in open networks based on unauthenticated encryption. Opportunistic Wireless Encryption.
- Increased key sizes with 192-bit sized keys. Only mandatory when certified as WPA3-Enterprise.

Additionally, WPA3 mandates the use of Protected Management Frames (PMF) which makes it impossible to launch de-authentication attacks. [18]

ARCHITECTURE & SPECIFICATION

Zero-Knowledge Proofs and WPA3

A zero-knowledge proof is a cryptographic protocol that enables one party to prove to another party that they know a value 'x' without conveying any information other than the fact that they know the value of 'x'.

WPA3 makes use of such a zero-knowledge proof to ensure that no secrets of the passwords are transmitted in the SAE handshake, but both handshake participants can be sure that the other party knows that they possess the same and correct password. In fact, both parties prove that they have knowledge over the same password. [18]

Modes Of Operation

WPA3 offers various modes to cater to different security needs -

1. *Personal Mode:* Uses SAE with no PSK and mandates PMF, providing strong security for home and small business networks. This mode replaces WPA2's Pre-Shared Key (PSK) mechanism with the Simultaneous Authentication of Equals (SAE) handshake, a password-authenticated key exchange based on the Dragonfly protocol. SAE ensures mutual authentication and prevents offline dictionary attacks by requiring active interaction for each password attempt. [19][20]
2. *WPA3-SAE-Transition Mode:* Allows for a gradual transition from WPA2 to WPA3 by supporting both SAE and PSK, with optional PMF.

3. *WPA3 Enterprise:* Similar to WPA2 Enterprise but with PMF enabled and enhanced security against KRACK attacks using CCMP with AES 128 encryption.
4. *WPA3 Enterprise Transition:* Allows for a smoother transition from WPA2 Enterprise to WPA3, supporting CCMP with AES 128 and optional PMF.
5. *WPA3 192-bit Mode:* Designed for high security environments, this mode uses GCMP with AES 256 and SHA 384 for key derivation, ensuring quantum safe security. [21]

Protected Management Frames (PMF)

A key architectural change is the mandatory use of Protected Management Frames (PMF), which safeguard against disassociation and deauthentication attacks that were common in WPA2. [22]

Wi-Fi uses three different frame categories- Management, Control, and Data. Management frames such as authentication, de-authentication, association, disassociation, beacons, and probe frames are used by wireless clients to find and connect to the right Wi-Fi network and manage the client connection after a successful association. Without the Protected Management Frames feature, all management frames are sent unprotected in the open. Transmitting open frames make connections vulnerable to attack. Protected Management Frames is a feature currently included in several Wi-Fi CERTIFIED programs that, when enabled, provides integrity protection for both unicast and broadcast management frames, and also encrypts unicast management frames in the same way as data to provide confidentiality. Based on the IEEE 802.11w amendment, Protected Management Frames utilizes the Security Association teardown protection mechanism already in place for encrypted data frames and therefore improves the resiliency of a Wi-Fi network. [23]

CONNECTING TO AN ACCESS POINT USING WPA3

WPA3 mandates support for the existing Simultaneous Authentication of Equals (SAE) handshake. This handshake is a Password Authenticated Key Exchange (PAKE), meaning authentication is performed based on a password. The SAE handshake provides forward secrecy and resistance against offline dictionary attacks and was added to the 802.11 standard in 2011. [24]

The output of WPA3's SAE handshake is a Pairwise Master Key (PMK), which is subsequently used to perform a 4-way handshake to derive a Pairwise Transient Key (PTK).
Even though WPA3 still uses WPA2's 4-way handshake, it is not vulnerable to dictionary attacks. This is because the PMK generated by the SAE handshake has much higher entropy than the password itself. Finally, in both modes, Protected Management Frames (PMF) must be used. Most notably, PMF prevents deauthentication attacks where an adversary forcibly disconnects victims from the AP. [24]

Understanding Figure 3 -

- *Discovery Phase: The Access Point broadcasts beacons containing its RSNE (Robust Security Network Element) with supported cipher suites, and the client selects an appropriate cipher.*
- *SAE Handshake: Both client and access point exchange Auth-Commit messages containing their scalar and element values (scal1, elem1 from client and scal2, elem2 from access point), which are derived from the shared password using elliptic curve cryptography. Both parties then independently derive the PMK (Pairwise Master Key) from these exchanged values. They exchange Auth-Confirm messages (conf1 and conf2) to mutually verify that both computed the same PMK, proving knowledge of the password without transmitting it.*
- *Association: After successful SAE authentication, the client sends an Association Request with its chosen RSNE and cipher, and the access point responds with an Association Response, establishing the connection parameters.*
- *4-Way Handshake: This phase derives session specific encryption keys. The access point sends Msg1 containing ANonce (a random nonce). The client derives the PTK (Pairwise Transient Key) from the PMK and nonces, then sends Msg2 with its SNonce, MIC (Message Integrity Code), and RSNE-Chosen confirmation. The access point derives the PTK, verifies the RSNE parameters, and sends Msg3 containing a MIC, its RSNE, and the GTK (Group Temporal Key) for multicast traffic. The client verifies the RSNE and sends Msg4 with a MIC to confirm completion. Once all verifications succeed, the secure connection is established with unique encryption keys for the session.*

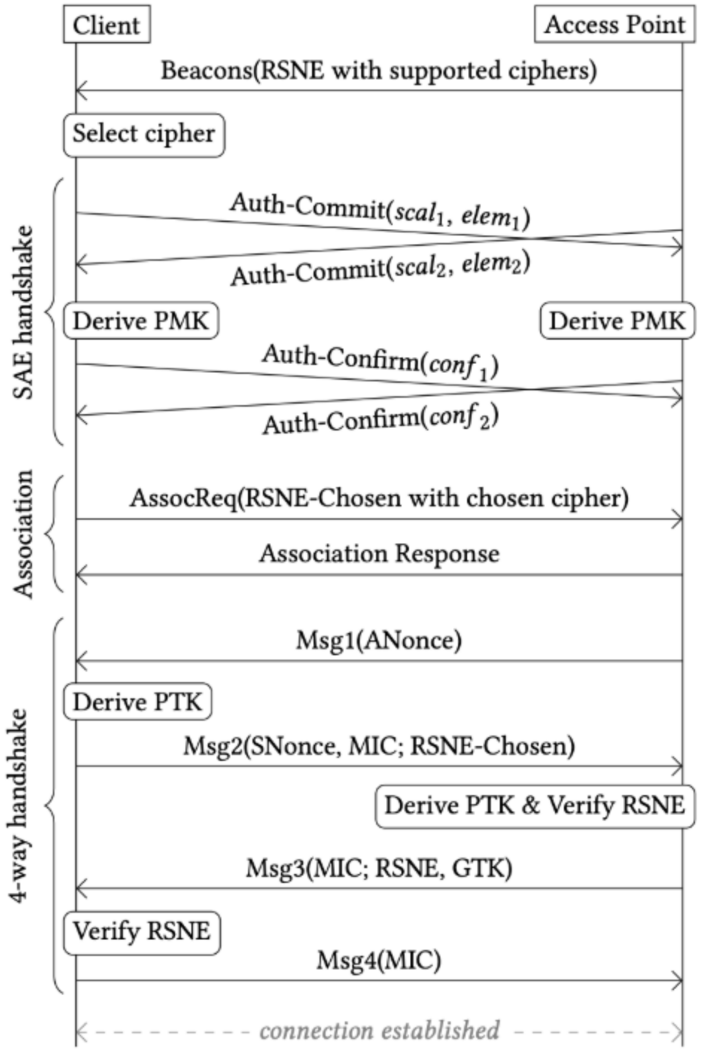


Figure 3: Connecting to an AP using WPA3. First the SAE handshake negotiates the master key (PMK), and then the 4-way handshake derives a session key (PTK). To support mesh networks, the SAE handshake was made so both parties can initiate it in parallel (hence the crossed arrows). [19]

SIMULTANOUS AUTHENTICATION OF EQUALS (SAE) PROTOCOL

With SAE, all elliptic curves are defined over the equation y^2 = x^3 + ax + b (mod p) where p is a prime and the values a, b, and p depend on the curve being used. We use G to denote the generator of a group, and q to denote the prime order of G. When executing the SAE handshake, the user readable password is converted into a group element. For MODP groups this is done using a hash to group algorithm, and for elliptic curves using a hash to curve algorithm. The resulting password element is denoted by P. [24]

The handshake itself is based upon the DragonFly Key Exchange Protocol and consists of a commit phase followed by a confirm phase. These two phases, along with the accompanying elliptic curve operations, are illustrated in Figure 4.

The handshake can be initiated concurrently by both participants (which may happen in mesh networks after connection loss). Nevertheless, in the more widely used infrastructure mode, the client will initiate the handshake by sending its commit frame, and subsequently the AP will reply using a commit and confirm frame. In turn the client sends it's confirm frame, completing the handshake.

Note*- When describing elliptic curve operations, we use lowercase letters to denote scalars (i.e. integers), and uppercase letters to denote elliptic curve points.

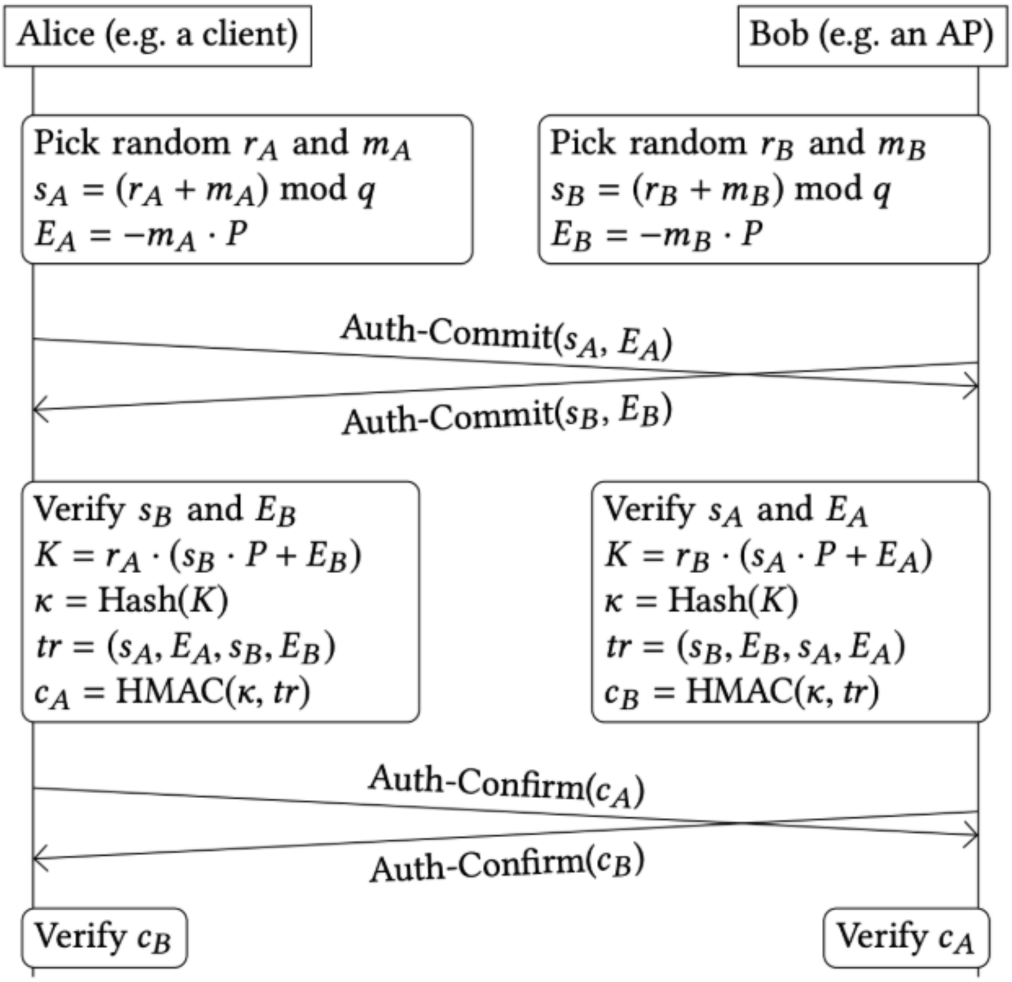

Alice (e.g. a client)
Bob (e.g. an AP)
Pick random r_A and m_A
$s_A = (r_A + m_A) \bmod q$
$E_A = -m_A \cdot P$
Pick random r_B and m_B
$s_B = (r_B + m_B) \bmod q$
$E_B = -m_B \cdot P$
Auth-Commit(s_A, E_A)
Auth-Commit(s_B, E_B)
Verify s_B and E_B
$K = r_A \cdot (s_B \cdot P + E_B)$
$\kappa = \text{Hash}(K)$
$tr = (s_A, E_A, s_B, E_B)$
$c_A = \text{HMAC}(\kappa, tr)$
Verify s_A and E_A
$K = r_B \cdot (s_A \cdot P + E_A)$
$\kappa = \text{Hash}(K)$
$tr = (s_B, E_B, s_A, E_A)$
$c_B = \text{HMAC}(\kappa, tr)$
Auth-Confirm(c_A)
Auth-Confirm(c_B)
Verify c_B
Verify c_A

Figure 4: SAE Handshake Commit & Confirm Phase [19]

Password Derivation Phase

The SAE Protocol begins with both peers converting the plaintext password into a Password Element (PE), a valid group element on the chosen elliptic curve or finite field. This is achieved through the hunting-and-pecking algorithm, which is a loop that repeatedly hashes the concatenation of the password, MAC addresses, and an iteration counter until a valid element is produced. This ensures that the mapping from password to group element is deterministic yet computationally infeasible to reverse. [17]

When constructing the commit frame, the pre-shared password is first converted into a curve point using a hash to curve algorithm. The specific algorithm used in SAE is based on a try and increment method, and is shown in figure 5. Summarized, it first hashes the password, together with a counter and the MAC addresses of both stations, and uses the output of the hash as the x-coordinate of the curve point. It then tries to find a solution for 'y' over the equation y^2 = x^3 +ax +b (mod p). In case a solution exists, the point (x,y) becomes the password element P. If no solution is found, the counter is increased, and another attempt is made to find a solution for 'y' using the new value for 'x'. Finally, to mitigate timing attacks, the main loop is always executed 'k' times, no matter when a solution for 'y' is found. In the extra iterations, calculations are based on a randomly generated password instead of the real one.

Layman Explanation for password derivation-

When a device connects to a WPA3 network, it needs to prove it knows the password without actually sending the password. This is important because if the password itself was sent (even encrypted), it could potentially be attacked. Instead, WPA3 uses mathematics to convert the password into a different form called a Password Element (PE) that can be used in calculations but doesn't reveal the password.

The Password Element is a point on something called an 'elliptic curve' think of it as a specific location on a complex mathematical curve. This point is calculated using-

- *Your password*
- *The MAC addresses of both your device and the router (unique hardware identifiers)*
- *A counter that increases until a valid point is found*
- *Hash functions that scramble the information*

The 'Hunting and Pecking' Process: The name hunting and pecking describes how the system searches for a valid point-

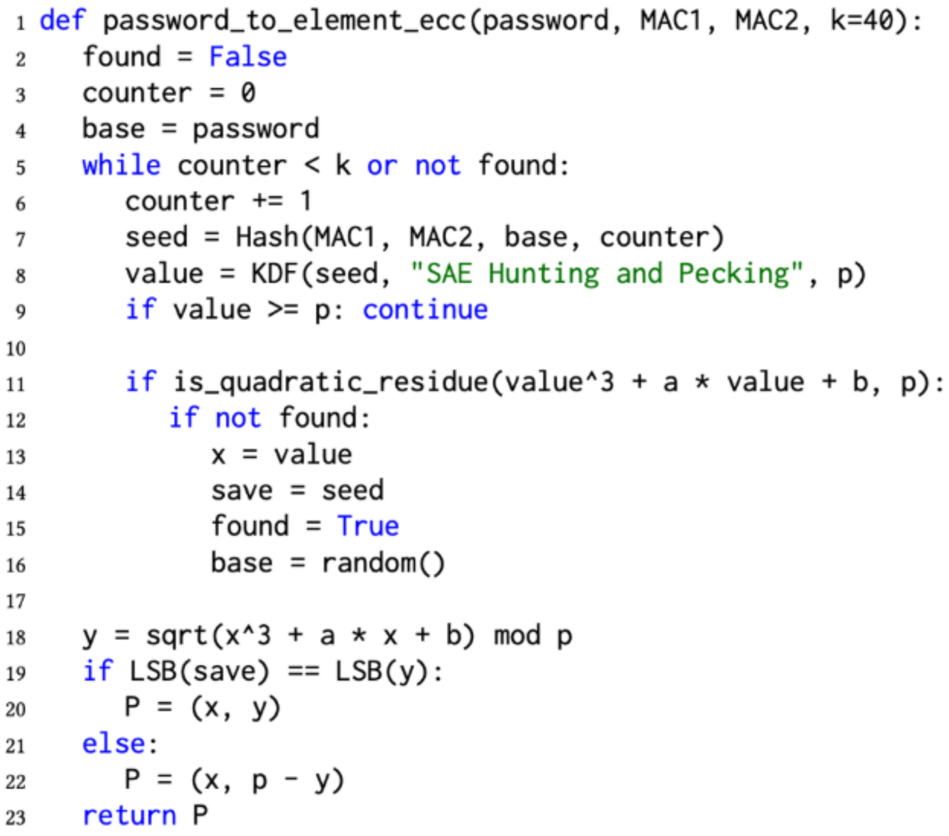
1. *It combines the password, MAC addresses, and a counter number.*
2. *It runs this through a hash function to get a random looking number.*
3. *It tries to use this number as an x-coordinate on the elliptic curve.*
4. *It checks if this x-coordinate corresponds to a valid point on the curve (by solving a mathematical equation).*
5. *If it doesn't work, it increases the counter and tries again.*
6. *This repeats until a valid point is found.*
7. *That valid point becomes the Password Element.*

Why it can't be reversed: This conversion is a 'one way function' - easy to go forward, nearly impossible to go backward. The following are the reasons why-

1. *Hash functions are one way**:** The process uses hash functions, which scramble data in a way that can't be unscrambled. It's like mixing paint colours, once you mix blue and yellow to get green, you can't separate them back into pure blue and yellow.*
2. *Multiple inputs mixed together**:** The Password Element is created from your password + MAC addresses + a counter. Even if someone had the Password Element, they wouldn't know which counter value was used, making it even harder to work backward.*
3. *Elliptic curve math is hard to reverse**:** Elliptic curve math is computationally hard to reverse due to the Elliptic Curve Discrete Logarithm Problem, making it practically impossible to derive the original values from a resulting curve point.*

Real World Analogy: Imagine you have a recipe that says 'add ingredients and bake'. You can easily make a cake by following the recipe. But if someone gives you only the finished cake, could you figure out the exact recipe, including the precise amounts of each ingredient? That would be very difficult or impossible. The Password Element is like the finished cake. You can make it from the password, but you can't reverse-engineer the password from it.

Why This Matters for Security: During the WPA3 handshake, your device and the router exchange information based on the Password Element, not the password itself. Even if an attacker captures all this information, they can't work backward to find your password. They can't test password guesses offline because they'd need to interact with your actual network to check if their guess produces the right Password Element.



```
def password_to_element_ecc(password, MAC1, MAC2, k=40):
  found = False
  counter = 0
  base = password
  while counter < k or not found:
    counter += 1
    seed = Hash(MAC1, MAC2, base, counter)
    value = KDF(seed, "SAE Hunting and Pecking", p)
    if value >= p: continue

    if is_quadratic_residue(value^3 + a * value + b, p):
      if not found:
        x = value
        save = seed
        found = True
        base = random()

  y = sqrt(x^3 + a * x + b) mod p
  if LSB(save) == LSB(y):
    P = (x, y)
  else:
    P = (x, p - y)
  return P
```

Figure 5: Converting the pre-shared password into an elliptic curve point in Python like pseudocode [24]

Understanding the code-

This code implements the 'Hunting and Pecking' algorithm for deriving an elliptic curve point from a password, MAC addresses, and parameters. It iterates up to k=40 times, incrementing a counter each iteration, and generates a seed by hashing MAC1, MAC2, a base value (initially the password), and the counter. The seed is processed through a KDF with the label 'SAE Hunting and Pecking' to produce a candidate x-coordinate (value). If this value passes a quadratic residue test (checking if x^3+ax+b is a quadratic residue (mod p), meaning a valid y-coordinate exists), the algorithm saves this x-coordinate and the corresponding seed, sets found=True, and randomizes base for security. It then computes y = sqrt(x^3+ax+b) mod p and constructs the final point P=(x,y) by selecting between 'y' and 'p-y' based on whether LSB(seed) equals LSB(y), ensuring deterministic point derivation. The function returns this elliptic curve point P, which is uniquely determined by the password, MAC addresses, curve parameters, and counter value at which a valid point was found.

Commit Phase

In the Commit Exchange, both sides commit to a single guess of the password. The peers generate a scalar and an element, exchange them with each other, and process the other's scalar and element to generate a common and shared secret. [18]

First, each peer generates two random numbers, private and mask that are each greater than one (1) and less than the order from the selected domain parameter set:

```
1 < private < q

1 < mask < q
```

These two secrets and the Password Element are then used to construct the scalar and element:

```
scalar = (private + mask) modulo q

Element = inverse(scalar-op(mask, PE))
```

If the scalar is less than two, the private and mask MUST be thrown away and new values generated. Once a valid scalar and Element are generated, the mask is no longer needed and MUST be irretrievably destroyed.

The peers exchange their scalar and Element and check the peer's scalar and Element, deemed peer-scalar and Peer-Element. If the peer has sent an identical scalar and Element i.e., if scalar equals peer-scalar and Element equals Peer-Element, it is sign of a reflection attack, and the exchange MUST be aborted.[18]

```
ss = F(scalar-op(private,

                    element-op(peer-Element,

                             scalar-op(peer-scalar, PE))))
```

To enforce key separation and cryptographic hygiene, the shared secret is stretched into two subkeys, a key confirmation key, kck, and a master key, mk. Each of the subkeys SHOULD be at least the length of the prime used in the selected group.[18]

```
kck | mk = KDF-n(ss, "Dragonfly Key Derivation")
```

where n = len(p)*2.

This results in both sides deriving an identical shared key without ever sending password-equivalent data. [21]

Layman Explanation-

The Commit Phase - 'Let's Create a Secret Together' - In the Commit phase, both your device and the router work together to create a shared secret without actually telling each other what it is. Here's how it works:

1. *Both sides start with the same Password Element (derived from your Wi-Fi password).*
2. *Each side generates two random numbers: one called 'private' and one called 'mask'.*
3. *Each side does some mathematical calculations using these random numbers and the Password Element.*
4. *They exchange the results of these calculations (called 'scalar' and 'Element').*
5. *Each side uses what they received + their own private random number to calculate a shared secret point called 'K'*

The main part is that even though they exchange information, the private random numbers are never shared. Because of complex math (elliptic curve cryptography), an attacker watching the exchange can't figure out these private numbers or the shared secret 'K'.

Why the Commit Phase Alone Isn't Enough: At the end of the Commit phase, both sides have calculated what they believe is the shared secret K. But there's a problem, how do they know they both calculated the SAME value? And what if -

- *One side made a calculation error?*
- *An attacker modified the messages in transit?*
- *Someone is pretending to know the password but doesn't?*

This is where the Confirm phase comes in.

Confirm Phase

In the Confirm Exchange, both sides confirm that they derived the same secret, and therefore, are in possession of the same password.

The Commit Exchange consists of an exchange of data that is the output of the random function, H(), the key confirmation key, and the two scalars and two elements exchanged in the Commit Exchange. The order of the scalars and elements are - scalars before elements, and sender's value before recipient's value.[18] So from each peer's perspective, it would generate:

```
confirm = H(kck | scalar | peer-scalar |

        Element | Peer-Element | <sender-id>)
```

The two peers exchange these confirmations and verify the correctness of the other peer's confirmation that they receive. If the other peer's confirmation is valid, authentication succeeds. If the other peer's confirmation is not valid, authentication fails.
If authentication fails, all ephemeral state created as part of the particular run of the Dragonfly exchange MUST be irretrievably destroyed. If authentication does not fail, ‘mk’ can be exported as an authenticated and secret key that can be used by another protocol, for instance IPsec, to protect other data. [18]

In the confirm phase, both peers derive a Key Confirmation Key (KCK) and Session Key from the shared secret using a key derivation function (KDF) based on HMAC-SHA256.
Each party then transmits an SAE Confirm message containing a Message Authentication Code (MAC) generated using the KCK, which authenticates the transcript and confirms both sides computed the same shared secret.
Successful confirmation establishes a Pairwise Master Key (PMK), which is subsequently used by WPA3’s internal 4-Way Handshake to derive traffic encryption keys. [21]

Layman explanation-

The Confirm Phase - ‘Let's Verify We Got the Same Secret’ - The Confirm phase is like a verification step. Here's what happens:

1. *Both sides take their shared secret ‘K’ and run it through a hash function to create a key (called κ - kappa).*
2. *Each side uses this key to create a special code (called a HMAC) that includes a summary of everything that happened in the Commit phase.*
3. *They exchange these codes.*
4. *Each side checks if the code they received matches what they expected.*

If the codes match, it proves three important things-

- *Both sides calculated the same shared secret ‘K’*
- *Both sides know the correct password (because that's how they got matching results).*
- *Nobody tampered with the messages during the Commit phase.*

If the codes don't match, the connection is immediately rejected, and they have to start over.

Why Both Phases Are Necessary-

- *Commit Phase: Creates the shared secret using the password and random values.*
- *Confirm Phase: Verifies both sides got the same result and proves mutual authentication.*

Security Benefits:

- *An attacker can't skip the Confirm phase because the verification would fail.*
- *An attacker can't modify messages in the Commit phase because the Confirm phase would detect it.*
- *Both sides prove they know the password without ever sending it.*
- *The two phase design provides multiple layers of security verification.*

SIMPLIFIED EXAMPLE OF DRAGONFLY HANDSHAKE USING ECC

Both parties Alice and Bob agree to a ECC E and to a prime p

Alice and Bob have a same password P

They derive a x-coordinate out of this password P with a hash function 'H()' and a key derivation function KDF(). They repeat this step until this x-coordinate is a valid quadratic residue mod p. This results in a valid point on the curve which is used as a generator G. In the dragonfly protocol this generator is also called PE password element. [18]

Then Alice and Bob generate two random numbers, private and mask.

These two random numbers and the password element are then used to construct the scalar and element:

scalar = (private + mask) modulo q

Element = inverse(scalar-op(mask, PE))

Alice and Bob exchange their scalar and Element and check that their peer's scalar and Element are valid.

Then Alice and Bob compute a shared secret similarly as in the ECDH:

K = private-op(peer-Element * (peer-scalar-op(PE)))

In the confirm exchange both parties confirm that they computed the same key K. [18]

This is essentially done with the hash function H() that is used to hash a part of the key K and confirming that both parties have the same hash. [18]

SECURITY IMPORVEMENTS OVER WPA2

WPA3 introduces several key security enhancements over WPA2, addressing major vulnerabilities that were exploited in previous generations of Wi-Fi security protocols.
The most significant change is the replacement of the Pre-Shared Key (PSK) mechanism with the Simultaneous Authentication of Equals (SAE) handshake. Unlike WPA2's PSK-based four-way handshake, which allows attackers to capture authentication frames and perform offline dictionary attacks, SAE requires an active interaction with the access point for every password attempt, effectively preventing large scale brute-force attacks.[17]

Provides Perfect Forward Secrecy

In WPA2, compromising the PSK exposes all past and future encrypted sessions. WPA3 resolves this by generating a unique session key for every authentication using ephemeral cryptographic values. Even if the password is later revealed, previous data transmissions remain secure. [24]

WPA3 ensures that compromise of long term secrets does not compromise past session keys. This is a critical property absent from WPA2 that WPA3 provides through the SAE handshake's design.

In each SAE handshake -

- Both parties generate fresh random values (private and mask) that are used only for that session. The shared secret K is computed from these ephemeral values combined with the Password Element. The Pairwise Master Key is derived from K, incorporating these random components After the session completes, the ephemeral values are irretrievably destroyed.

  Even if an attacker later obtains the password, they cannot reconstruct past sessions because -

  - The random private and mask values no longer exist
  - These values were never transmitted over the air
  - Without these values, the shared secret K cannot be recomputed
  - Without K, past PMKs and PTKs cannot be derived

Key Reinstallation Attack (KRACK) Prevention

The confirm phase of the SAE handshake ensures mutual key confirmation, eliminating the vulnerability exploited by KRACK that affected WPA2's four-way handshake. The SAE confirm phase, creates a cryptographic binding of all handshake messages using a hash based Message Authentication Code computed over the entire transcript. Any attempt to replay or manipulate messages causes confirm verification to fail and aborts authentication. [19]

Prevention of De-authentication and Frame Injection Attacks

WPA3 makes Protected Management Frames (PMF) mandatory, addressing a critical vulnerability in WPA2 where management frames (authentication, deauthentication, association, disassociation) were transmitted unencrypted and unauthenticated. This allowed attackers to forge deauthentication frames to forcibly disconnect clients, enabling denial-of-service attacks, facilitating handshake capture for offline cracking, and supporting evil twin attacks. With PMF enabled, unicast management frames are encrypted using the same Pairwise Transient Key (PTK) used for data frames, while broadcast management frames are authenticated using the Broadcast Integrity Protocol (BIP), ensuring any forged or manipulated frames are detected and dropped. This protection maintains stable connections even in the presence of attackers attempting to disrupt network operations through management frame manipulation. [21]

KNOWN VULNERABILITIES AND LIMITATIONS OF WPA3

While WPA3 addresses fundamental WPA2 vulnerabilities, it is not without its own security challenges. The 2019 Dragonblood research identified multiple vulnerabilities in WPA3 implementations, including side channel attacks, downgrade attacks, group negotiation weaknesses, and denial-of-service vectors. This section focuses on two critical downgrade related vulnerabilities that exploit WPA3's backward compatibility mechanisms.

Downgrade & Dictionary Attacks

In the transition mode of WPA3, an AP accepts connections using WPA3-SAE and WPA2 with the same password. This provides compatibility with older clients, while WPA2's 4-way handshake detects downgrade attacks. That is, if an adversary modifies beacons to trick the client into thinking the AP only supports WPA2, the client will detect this downgrade attack during WPA2's 4-way handshake. This is because the 4-way handshake contains an authenticated RSNE element listing the AP's supported cipher suites, allowing a client to detect if an adversary forged the RSNEs in beacons. This means WPA3 provides forward secrecy, even when using the transition mode of WPA3-SAE. [19]

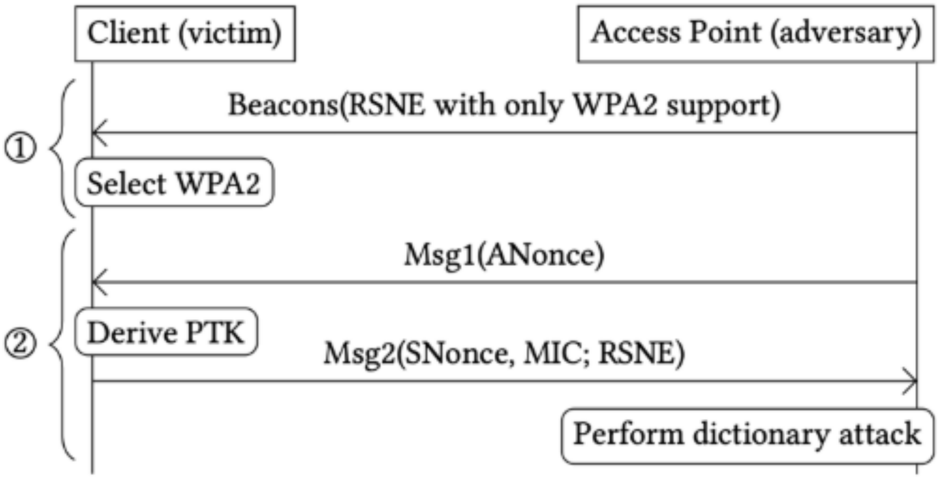


Figure 6: Dictionary attack against WPA3-SAE when it is operating in transition mode, by attempting to downgrade the client into directly using WPA2's 4-way handshake. [19]

The problem is that, although downgrade attacks are detected by WPA2's 4-way handshake, by that point an adversary has captured enough data to perform a dictionary attack. This is because an adversary only needs to capture a single authenticated 4-way handshake message to carry out a dictionary attack [19]. Moreover, a man-in-the-middle position is not needed to carry out the attack. The only requirements are that we know the SSID of the network, and that we are close to a client. If these conditions are met, the adversary can broadcast a WPA2-only network with the given SSID (stage -1 in Fig. 6). This causes the client to connect to our rogue AP using WPA2. The adversary can forge the first message of the 4-way handshake, since this message is not authenticated. In response, the victim will transmit message 2 of the 4-way handshake, which is authenticated. Based on this authenticated handshake message, a dictionary attack can be carried out. [19]

SAE Group Negotiation Attack

The SAE handshake can be run using different elliptic curve or multiplicative groups mod p (i.e. ECP or MODP groups). The 'Group Description' gives an overview of supported groups. Additionally, the 802.11 standard allows station to prioritize groups in a user configurable order. Although this provides flexibility, it requires a secure method to negotiate the group that will be used. Unfortunately, the mechanism that negotiates which group or curve is used during the SAE handshake is trivial to attack. [19]

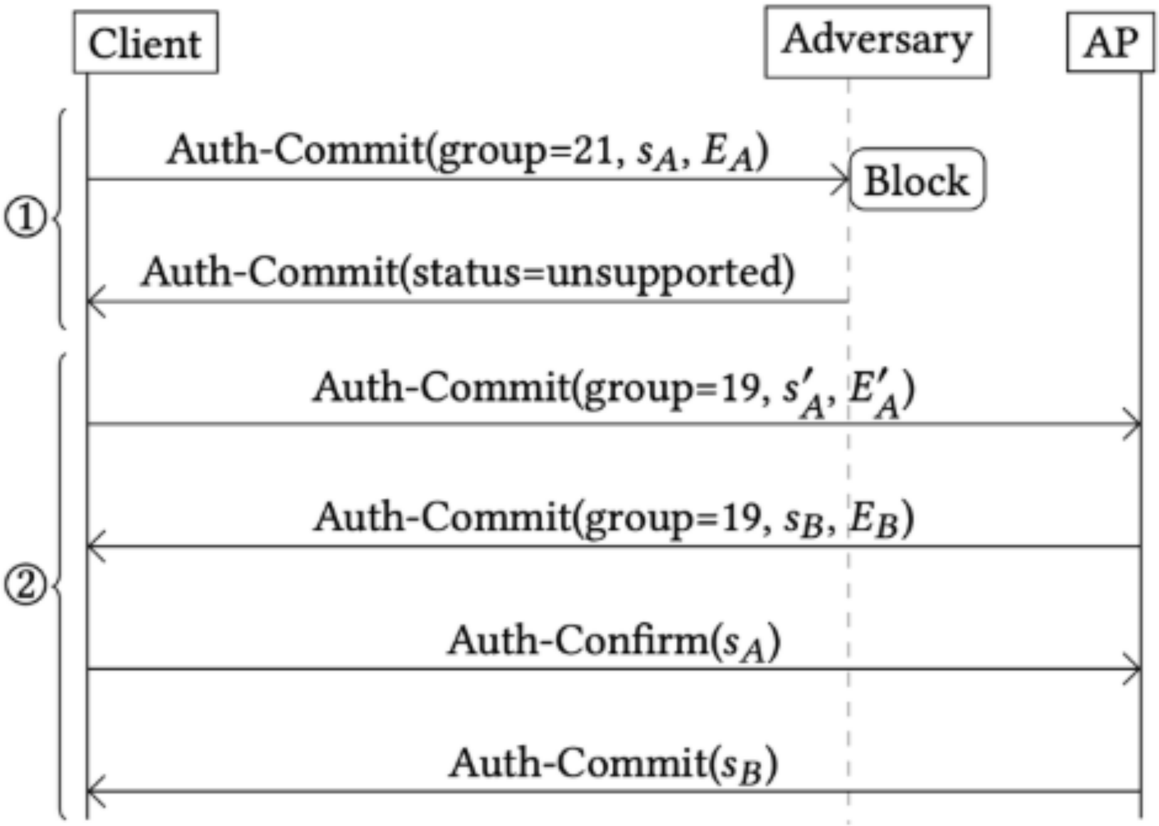

Client
Adversary
AP
①
Auth-Commit(group=21, s_A, E_A)
Block
Auth-Commit(status=unsupported)
②
Auth-Commit(group=19, s'_A, E'_A)
Auth-Commit(group=19, s_B, E_B)
Auth-Confirm(s_A)
Auth-Commit(s_B)

Figure 7: Downgrade attack against SAE's group selection: a man-on-the-side can force the client (initiator) into using a different cryptographic group during the SAE handshake. [24]

With SAE, the used group is negotiated as follows –

When a client connects to an AP, it includes its desired group in the commit frame, along with a valid scalar 'si' and element 'Ei' . In case the AP does not support this group, it will reply using a commit frame with a status field equal to 'unsupported finite cyclic group' (see stage -1 in Figure 7). In turn the client will attempt to use its next preferred group, and send a new commit frame with this group, and corresponding new scalar 'si' and element 'Ei' .This process continues until the client selected a curve that the AP supports.

Unfortunately, there is no mechanism that detects if someone interfered with this process. This makes it trivial to force the client into using a different group. [19]

Simply forge a commit frame that indicates the AP does not support the currently selected group. Figure 7 illustrates the resulting downgrade attack. Here the client first constructs a commit frame requesting group 21 (i.e. curve P-521). However, the adversary blocks this frame from arriving at the AP (see stage ○1 in Figure 5). This can be accomplished by jamming the frame, or by forging channel switch announcements. The adversary then forges a commit frame that indicates the AP does not support the request group. In response, the client will pick its second preferred group, which in our example is group 19 (i.e. curve P-256). From this point onwards, a normal SAE handshake is executed using group 19 (see stage -2 in Figure 7). Notice that this negotiation process is never cryptographically validated, meaning the downgrade attack is not detected. It is also possible to perform an upgrade attack, where the victim is forced to use a more secure cryptographic group. That is, if the victim prefers small cryptographic groups, our attack can force the victim into using bigger groups. This may be useful when performing denial-of-service attacks, or to amplify timing side channels. [24]

Conclusion:

The evolution from WPA2 to WPA3 represents a major improvement in Wi-Fi security. While WPA2 introduced strong encryption and authentication, vulnerabilities like KRACK exposed risks such as key reinstallation and offline dictionary attacks. WPA3 addresses these issues through the Simultaneous Authentication of Equals (SAE) handshake, providing perfect forward secrecy, mutual authentication, and mandatory protected management frames. Although some implementation challenges and downgrade attacks still exist, WPA3 ensures that shared secrets are never transmitted, session keys are unique for each connection, and past communications remain secure even if passwords are compromised, making modern Wi-Fi networks much more resilient against sophisticated attacks.

Bibliography

[1] B Indira Reddy & V. Srikanth, “Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3)”, July 2019, [Online]. Available: https://www.researchgate.net/publication/334445004_Review_on_Wireless_Security_Protocols_WEP_WPA_WPA2_WPA3

[2] S Vibhuti, “IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability”, 2005, [Online]. Available: https://www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf

[3] M Khasawneh et al., “A Survey on Wi-Fi Protocols: WPA and WPA2”, March 2014, [Online]. Available: https://www.researchgate.net/publication/290743584_A_Survey_on_Wi-Fi_Protocols_WPA_and_WPA2

[4] Michael, M., “Wireless encryption basics. University of Wollongong”, 2005 [Online]. Available: https://documents.uow.edu.au/~jennie/WEB/WEB05/Michael.pdf

[5] ERT-EU, “Wi-Fi Protected Access II (WPA2) handshake vulnerabilities (CERT-EU Security Advisory 2017-021)”, 2017, [Online]. Available: https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-021.pdf

[6] National Institute of Standards and Technology (NIST), “IEEE 802.11i overview”, 2001, [Online]. Available: https://csrc.nist.rip/archive/wireless/S10_802.11i%20Overview-jw1.pdf

[7] Study CCNA, “802.1X authentication explained. Study CCNA”, [Online]. Available: https://study-ccna.com/802-1x-authentication/

[8] Control Engineering, “Wireless security: IEEE 802.11 and CCMP AES. Control Engineering”, [Online]. Available: https://www.controleng.com/wireless-security-ieee-802-11-and-ccmp-aes/

[9] Mostafa, A. “ What WPA3 brings to Wi-Fi: Focus on SAE and OWE. CWNP”, 2022, [Online]. Available: https://www.cwnp.com/uploads/what-wpa3-brings-to-wi-fi-focus-on-sae-and-owe-ahmed-mostafa-cwne-candidate-article-2022.pdf

[10] Changhua He & John C Mitchell, “Analysis of the 802.11i 4-Way Handshake”, 2004, [Online]. Available: https://cs.stanford.edu/people/jcm/papers/fp09-he.pdf

[11] IEEE Std 802.11i-2004, IEEE Standard for Information Technology, Telecommunications and Information Exchange Between Systems, Local and Metropolitan Area Networks, Specific Requirements-Part 11: Wireless LAN MAC and PHY Specifications—Amendment 6: MAC Security Enhancements, IEEE Computer Society, 2004. [Online]. Available: https://standards.ieee.org/standard/802_11i-2004.html

[12] EE Times, "IEEE 802.11i and wireless security," 2014. [Online]. Available: https://www.eetimes.com/ieee-802-11i-and-wireless-security/

[13] NIST, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality," NIST SP 800-38C, May 2004. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-38c/final

[14] CERT-EU, "KRACK – Key Reinstallation Attacks: Breaking WPA2," 2017. [Online]. Available: https://cert.europa.eu/publications/security-advisories/2017-021/

[15] KRACK Attacks, "Breaking WPA2," 2017. [Online]. Available: https://www.krackattacks.com/

[16] Vanhoef, M., & Piessens, KRACK: Key Reinstallation Attacks on WPA2. University of Leuven, 2017 [Online]. Available: https://papers.mathyvanhoef.com/ccs2017.pdf

[17] RFC 7664 (Internet Engineering Task Force 'IETF') "DragonFly Key Exchange Protocol" November 2015. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7664

[18] Humboldt University Berlin "WPA3 DragonFly Handshake" [Online]. November 2018 Available: https://sarwiki.informatik.hu-berlin.de/WPA3_Dragonfly_Handshake

[19] Mathy Vanhoef and Eyal Ronen (International Association for Cryptologic Research 'IACR') "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd" May 2020. [Online]. Available: https://eprint.iacr.org/2019/383.pdf

[20] RFC 7664 (Internet Engineering Task Force 'IETF') "DragonFly Key Exchange Protocol" November 2015. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7664

[21] Wi-Fi Alliance (Wi-Fi ORG) "WPA3 Specification v3.5" February 2025. [Online]. Available: https://www.wi-fi.org/system/files/WPA3%20Specification%20v3.5.pdf

[22] CISCO "WPA3 Deployment Guide" October 2025. [Online]. Available: https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/technical-reference/wpa3-deployment-guide.pdf

[23] Philippe Ebbecke (Wi-Fi Alliance) "Protected Management Frames enhance Wi-Fi network security" [Online]. Available: https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security

[24] Mathy Vanhoef and Eyal Ronen (AirCrack-ng ORG) "Dragonblood: A Security Analysis of WPA3's SAE Handshake" [Online]. Available: https://dl.aircrack-ng.org/wiki-files/doc/additional_papers/dragonblood.pdf

[25] Cosmin Cazan and Mohammad Y Mansour (Intel), "Seamless Next-generation Wi-Fi Security Through Multivendor End-to-end WPA3 Verification" Nov. 2021. (white Paper) [Online]. Available: https://www.intel.com/content/www/us/en/content-details/841026/seamless-next-generation-wi-fi-security-through-multivendor-end-to-end-wpa3-verification-white-paper.html

[26] Mathy Vanhoef (Wi-Fi Alliance) "WPA3 Security Considerations" November 2019. [Online]. Available: https://wpa3.mathyvanhoef.com/WPA3_Security_Considerations_201911.pdf

ANNEXURE-I

Authentication & Key Exchange Terms -

ANonce (Authenticator Nonce): A random number generated by the Access Point during the 4-Way Handshake. Used along with SNonce and other parameters to derive the PTK.

SNonce (Station Nonce): A random number generated by the client device (station) during the 4-Way Handshake. Combined with ANonce to create unique session keys.

KEK (Key Encryption Key): A key derived from the PTK used to encrypt the GTK and other key data during the 4-Way Handshake.

TK (Temporal Key) The actual encryption key derived from the PTK and used for encrypting data frames during a Wi-Fi session.

802.1X A port-based network access control framework used in Enterprise Wi-Fi networks to authenticate users through an external server like RADIUS before granting network access.

PSK (Pre-Shared Key) The Wi-Fi password that both the client device and access point know in advance. In WPA2, this password is used directly to derive encryption keys.

SAE (Simultaneous Authentication of Equals) The new authentication handshake used in WPA3, also known as Dragonfly. Unlike WPA2, both the client and access point are "equals" in the authentication process, and neither acts purely as a server or client.

PAKE (Password Authenticated Key Exchange) A type of cryptographic protocol that allows two parties to establish a shared secret key based on a password, while protecting against offline password guessing attacks.

Dragonfly The name of the key exchange protocol underlying SAE. It uses elliptic curve cryptography to prevent attackers from testing password guesses offline.

Four-Way Handshake The authentication process used in WPA2 (and still used in WPA3 after SAE). It consists of four messages exchanged between client and access point to establish encryption keys. In WPA2, this handshake is vulnerable to offline dictionary attacks.

Handshake The initial exchange of messages between a client device and access point when connecting to Wi-Fi. This exchange proves both parties know the correct password and establishes encryption keys for the session.

Cryptographic Concepts -

PRF (Pseudo-Random Function) A cryptographic function that takes several inputs (PMK, nonces, MAC addresses) and produces the PTK in a deterministic but unpredictable way.

Replay Counter A sequential number used to prevent replay attacks by ensuring each message is only processed once. If an attacker resends an old message, the replay counter will reveal it.

LSB (Least Significant Bit) The rightmost bit in a binary number. Used in the hunting and-pecking algorithm to deterministically select between two possible y-coordinates on an elliptic curve.

PMK (Pairwise Master Key) The master key derived from the authentication process. In WPA2, this is derived directly from the password. In WPA3, it's derived from the SAE handshake and includes random ephemeral values.

PTK (Pairwise Transient Key) The session key derived from the PMK that is actually used to encrypt data during a Wi-Fi session. This key is temporary and unique to each connection session.

GTK (Group Temporal Key) The key used to encrypt broadcast and multicast traffic sent to all devices on the network.

KCK (Key Confirmation Key) A key derived during the SAE handshake used to generate Message Authentication Codes that prove both parties computed the same shared secret.

Password Element (PE) In SAE, the password is converted into a mathematical point on an elliptic curve called the Password Element. This conversion is done using the hunting-and-pecking algorithm.

Ephemeral Values Temporary random numbers generated fresh for each session that are used in cryptographic operations and then immediately destroyed. These provide forward secrecy because they cannot be reconstructed later.

Extensible Authentication Protocol (EAP) It is a framework for network authentication that supports a variety of authentication methods, such as passwords, certificates, or tokens.

Mathematical notations in Figure 2:

Mathematical Concept	Symbol/Notation	Layman's Explanation	Purpose in WPA3 SAE
Scalar	S (e.g., s_A)	Just a number (or multiplier). It's a random, non-secret value that is calculated and shared during the Commit Phase.	Used as a multiplier in the calculation to derive the final secret key K.
Element	E (e.g., E_A)	A point on the Elliptic Curve. This is a partial, scrambled calculation result that is safely shared.	Used as a key component for point addition in the final formula to derive K.
Scalar Multiplication	. (dot)	Multiplying a point by a number. This is *not* normal multiplication; it means adding the point to itself 'n' times on the curve.	This complex operation makes it computationally infeasible for an attacker to figure out the number r used to multiply the point P
Point Addition	+(plus)	Combining two points on the Elliptic Curve to find a third point. It involves unique rules based on the curve's geometry.	Used to combine the shared Element E with the product of the scalar and the Password Element.
Point Negation	- (minus)	The opposite point on the curve. Mathematically, it's finding a point that, when added to the original, results in the "point at infinity."	Used as a necessary step in the calculation (-m_A x P) to correctly isolate the values needed for the final shared secret K.

Mathematical Concept	Symbol/Notation	Layman's Explanation	Purpose in WPA3 SAE
Password Element	P	A specific, fixed point on the curve that both devices calculate from the password.	Serves as the *foundation* or starting point for all cryptographic operations in the handshake.
Shared Secret	K	The final, identical point that both devices arrive at. This point becomes the Pairwise Master Key (PMK).	Proves that both devices know the correct password, and its high entropy provides the session's encryption keys.

Encryption & Integrity -

TKIP (Temporal Key Integrity Protocol) An encryption protocol used in WPA that built upon WEP's RC4 cipher but added per-packet key mixing and message integrity checks. Considered weak and replaced by CCMP in WPA2.

MIC (Message Integrity Check) - WPA/TKIP Also called "Michael" in WPA, a keyed hash function used to ensure packet integrity and prevent tampering. Weaker than the integrity protection in CCMP.

CBC-MAC (Cipher Block Chaining Message Authentication Code) A cryptographic technique used in CCMP to provide data integrity and authenticity verification alongside encryption.

CTR (Counter Mode) An encryption mode that turns a block cipher like AES into a stream cipher for faster encryption. Used in CCMP alongside CBC-MAC.

MPDU (MAC Protocol Data Unit) The data payload and certain header fields that are protected by CCM encryption in WPA2 and WPA3.

CRC-32 (Cyclic Redundancy Check) A weak integrity check used in WEP that could be easily manipulated by attackers. Replaced by MIC in WPA and CBC-MAC in WPA2.

Network & Protocol Terms -

RSN (Robust Security Network) A wireless network that implements the full IEEE 802.11i security standard, requiring strong authentication and encryption before allowing data traffic.

Pairwise Key Hierarchy The set of keys used to protect unicast (one-to-one) communication between a specific client and the access point.

Group Key Hierarchy The set of keys used to protect multicast and broadcast traffic sent from the access point to multiple clients simultaneously.

Open System Authentication (OSA) A WEP authentication method where the access point grants access based on SSID matching without requiring encryption credentials.

Shared Key Authentication (SKA) A WEP authentication method using a four-step challenge-response process where the client encrypts a challenge with the shared WEP key.

Infrastructure Mode The standard Wi-Fi network configuration where clients connect through an access point rather than directly to each other.

Mesh Networks A network topology where devices connect directly to multiple other devices, creating redundant paths. SAE was designed to support concurrent handshake initiation for mesh scenarios.

Channel-Switch Announcement A management frame that tells clients to switch to a different Wi-Fi channel. Can be forged by attackers to facilitate downgrade attacks.

WEP-Related Terms -

WEP (Wired Equivalent Privacy) The original Wi-Fi security protocol from 1997, now deprecated due to critical vulnerabilities in its RC4 encryption and short initialization vectors.

WEP-40 / WEP-128 Versions of WEP with different key lengths: 40-bit (plus 24-bit IV) and 104-bit (plus 24-bit IV) secret keys.

IV (Initialization Vector) - WEP A 24-bit value used in WEP encryption. The short length meant IVs were frequently reused, allowing attackers to crack the encryption.

Attack Types -

Frame Size Leakage A side-channel vulnerability where packet size and timing patterns can reveal information even when content is encrypted, potentially enabling targeted attacks.

Replay Attack An attack where captured network packets are retransmitted to trick the system into accepting old data or reusing encryption keys.

Packet Injection An attack technique where malicious data packets are inserted into network traffic to compromise security or manipulate communications.

Eavesdropping Passive monitoring and interception of network communications without the knowledge of the communicating parties.

Password Guessing An attack method where the attacker systematically tries different password combinations to gain unauthorized access.

Nonce Reuse A critical security failure where the same nonce is used more than once with the same encryption key, breaking encryption security. Exploited in KRACK attacks.

Key Reinstallation The core vulnerability in KRACK where retransmitted handshake messages cause a device to reinstall already-in-use encryption keys, resetting security parameters.

Deauthentication Attack An attack where forged deauthentication frames forcibly disconnect clients from an access point, enabling handshake capture or denial of service.

Disassociation Attack Similar to deauthentication attacks but targeting the association state between client and access point.

WPA3-Specific Terms -

OWE (Opportunistic Wireless Encryption) A WPA3 feature that provides encryption for open (passwordless) networks like those in airports or cafes, preventing eavesdropping without requiring user authentication.

Wi-Fi CERTIFIED Easy Connect A WPA3 program that provides a straightforward method to securely add devices to a network, often using QR codes.

Commit Phase The first phase of the SAE handshake where both parties exchange scalars and elements to begin establishing a shared secret.

Confirm Phase The second phase of the SAE handshake where both parties verify they computed the same shared secret through cryptographic confirmation.

Hash-to-Curve Algorithm An algorithm used in SAE to convert a password into a valid point on an elliptic curve, implemented through the hunting-and-pecking method.

Try-and-Increment Method The approach used in the hunting-and-pecking algorithm that repeatedly tries different x-coordinates until finding one that corresponds to a valid curve point.

Group Description Documentation specifying which elliptic curve or multiplicative groups are supported for the SAE handshake.

Cryptographic Operations -

Scalar-op Scalar multiplication operation in elliptic curve cryptography, where a point is added to itself multiple times.

Element-op Point addition operation in elliptic curve cryptography, combining two curve points to produce a third point.

Inverse Operation A mathematical operation that reverses another operation, used in SAE to compute elements from scalars and the password element.

KDF-n (Key Derivation Function with output length n) A key derivation function that produces an output of specified length n, used in SAE to derive the KCK and master key from the shared secret.

Quadratic Residue Test A mathematical test to determine if a value can produce a valid y-coordinate on an elliptic curve, used in the hunting-and-pecking algorithm.

Point at Infinity The identity element in elliptic curve addition, analogous to zero in regular arithmetic. Used conceptually in point negation.

Elliptic Curve Cryptography (ECC) A type of public-key cryptography based on the mathematical properties of elliptic curves. WPA3's SAE uses ECC because it provides strong security with smaller key sizes compared to traditional methods.

Scalar In elliptic curve cryptography, a scalar is an integer (whole number) used in mathematical operations. In SAE, scalars are random secret values used in the commit phase.

Element In elliptic curve cryptography, an element is a point on the elliptic curve. In SAE, elements are derived from scalars and the Password Element and exchanged between client and access point.

Discrete Logarithm Problem A hard mathematical problem: given G, P, and the result of scalar multiplication (e.g., k × G = P), it's computationally infeasible to find the scalar k. WPA3's security relies on this difficulty.

Standards & Organizations -

IEEE 802.11 Standard The family of technical specifications defining wireless local area networks (WLANs), including security protocols.

NIST (National Institute of Standards and Technology) U.S. government agency that approved AES as the encryption standard used in Wi-Fi security.

Wi-Fi Alliance Industry organization that creates Wi-Fi certification programs including WPA, WPA2, and WPA3.

ACM Conference on Computer and Communications Security Academic conference where KRACK attack details were first presented in November 2017.

US-CERT United States Computer Emergency Readiness Team, the security organization that coordinated KRACK vulnerability disclosure.

Implementation Terms -

wpa_supplicant A widely-used Wi-Fi client software implementation for Linux and Android. Had a critical bug making devices vulnerable to installing all-zero encryption keys in KRACK attacks.

All-Zero Encryption Key A catastrophic vulnerability where the encryption key is set to all zeros, effectively nullifying all security. Affected about half of Android devices in KRACK attacks.

Transcript The complete record of all messages exchanged during a cryptographic handshake, used in verification and authentication.

Status Field A field in SAE commit frames indicating whether a requested cryptographic group is supported, exploitable in downgrade attacks.

Cipher Suite A combination of cryptographic algorithms used together (encryption algorithm, key exchange method, authentication method, etc.).

Security Concepts -

Mutual Authentication A security property where both parties in a communication prove their identities to each other, not just one-way authentication.

Freshness The property ensuring that cryptographic values like nonces and keys are newly generated and haven't been reused from previous sessions.

Forward Secrecy: It ensures that even if a hacker later obtains a network's private key, they cannot decrypt past sessions. WPA3 implements this feature through its Simultaneous Authentication of Equals (SAE) protocol, which generates unique session keys for every connection. This prevents previously recorded data from being exposed in the future.

Cryptographic Binding Creating a mathematical link between messages to ensure they belong together and haven't been tampered with or substituted.

Key Separation The security principle of using different keys for different purposes (e.g., separate keys for encryption vs. authentication).

Cryptographic Hygiene Best practices in using cryptographic systems, such as proper key management, avoiding key reuse, and secure random number generation.

Accountability In Enterprise mode, the ability to track which specific user performed which actions on the network, enabled by individual credentials.

Attack Vectors & Vulnerabilities -

Side-Channel Leak Information unintentionally revealed through implementation details like timing, power consumption, or cache access patterns rather than the cryptographic algorithm itself.

Packet Loss Normal wireless communication issue where transmitted packets fail to reach their destination, requiring retransmission. Exploited in KRACK attacks.

Wireless Proximity The physical distance requirement for Wi-Fi attacks, typically within the same radio range (tens to hundreds of meters).

Rogue AP (Rogue Access Point) A fake access point set up by an attacker to trick users into connecting, used in downgrade and evil twin attacks.

Forged Frame A network packet crafted by an attacker to appear as if it came from a legitimate source, used in various Wi-Fi attacks.

Passive Attack An attack where the attacker only observes and records network traffic without actively transmitting, making it undetectable.

Active Attack An attack requiring the attacker to transmit packets or interact with the network, making it potentially detectable and preventable.

Research & Disclosure -

Coordinated Disclosure The practice of privately informing affected vendors of vulnerabilities before public announcement, allowing time to develop patches.

Vanhoef and Piessens Belgian researchers from University of Leuven who discovered the KRACK vulnerability in WPA2 in 2016.

Vanhoef and Ronen Researchers who discovered the Dragonblood vulnerabilities in WPA3 in 2019.

Dragonblood Research The 2019 study that identified multiple vulnerabilities in WPA3 implementations, including side-channel attacks and downgrade weaknesses.

Network Configuration Terms -

Mixed Mode A network configuration allowing both old and new security protocols for compatibility, creating potential security vulnerabilities.

Fallback Mechanism A system's ability to revert to older, often weaker protocols when newer ones fail, exploitable by attackers.

Transition Mechanism Features designed to help networks migrate from older to newer security protocols while maintaining compatibility.

Group Negotiation Process The exchange of messages between client and access point to agree on which cryptographic group to use, vulnerable to manipulation in WPA3.

Unicast Frame A network packet sent from one device to a specific single destination device.

Multicast Frame A network packet sent from one device to multiple specific destination devices simultaneously.

Broadcast Frame A network packet sent from one device to all devices on the network.

Miscellaneous Technical Terms -

Radio Waves Electromagnetic waves used to transmit Wi-Fi signals, allowing wireless communication but also making networks accessible to anyone in range.

Jamming Using radio interference to deliberately block or disrupt wireless communications, used in some sophisticated attacks.

Man-on-the-Side A network position where the attacker can observe and inject packets but is not directly between the communicating parties.

Sender-ID An identifier included in SAE confirm messages to specify which party sent the messageIteration Counter A value incremented during the hunting-and-pecking algorithm to generate different candidate password elements.

Base Value The initial input (password) used in the hunting-and-pecking algorithm, randomized in extra iterations to prevent timing attacks.

Ephemeral State Temporary cryptographic values and session data that must be securely destroyed after use to maintain forward secrecy.

Certificate A digital document that proves the identity of a user or device, used in Enterprise mode authentication.

Smart Card A physical security device containing digital certificates and cryptographic keys, used in advanced Enterprise authentication.

Multi-Factor Authentication A security system requiring multiple forms of proof of identity (e.g., password + code from phone), supported in Enterprise mode.

Suite B Cryptography NSA-approved cryptographic algorithms used in WPA3-Enterprise 192-bit mode for protecting classified information.

Quantum-Safe Security Cryptographic approaches designed to resist attacks from quantum computers, claimed for WPA3 192-bit mode.