
WPA/WPA2/WPA3

WPA-
WI-FI PROTECTED ACCESS

- What is WPA?
- Why WPA? -- Background of WEP
- How WPA works? -- Encryption and Authentication
- What's next?

WPA- WIFI PROTECTED ACCESS

WPA and its background

- WPA is a security standard for wireless network devices.
- It is a security protocol or also known as encryption protocol which was created to take the place of the Wired Equivalent Privacy (WEP) or to develop upon the features of WEP for Wi-Fi networks.
- In 2003, it was launched with the 802.11i wireless standard.

WEP (Wired Equivalent Privacy) was an early encryption protocol for wireless networks, designed to secure WLAN connections prior WPA. WEP used the RC4 algorithm for encrypting data, creating a unique key for each packet by combining a new Initialization Vector (IV) with a shared key. IV is a 24-bit pseudo-random number used to create a 64-bit key by concatenating it with a shared-secret key, which is 40 bits in length. Decryption involved reversing this process, using the IV and the shared key to generate a key stream and decrypt the payload.

WHAT'S WRONG WITH WEP?

- Weak Encryption (RC4)
- Weak Shared key authentication
- Weak message integrity Checking with CRC-32
- Initialization vector is too small and in clear text

And thus, WPA, launched in 2003, emerged as an effective successor to WEP, addressing its flaws. WPA uses the temporal key integrity protocol (TKIP) encryption to improve key management and integrity checks.

WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

WPA has two modes: WPA-Personal for home networks and WPA-Enterprise for enterprises that use RADIUS servers

WPA AUTHENTICATION

Pre-Shared Key (PSK) Authentication (Personal Mode)

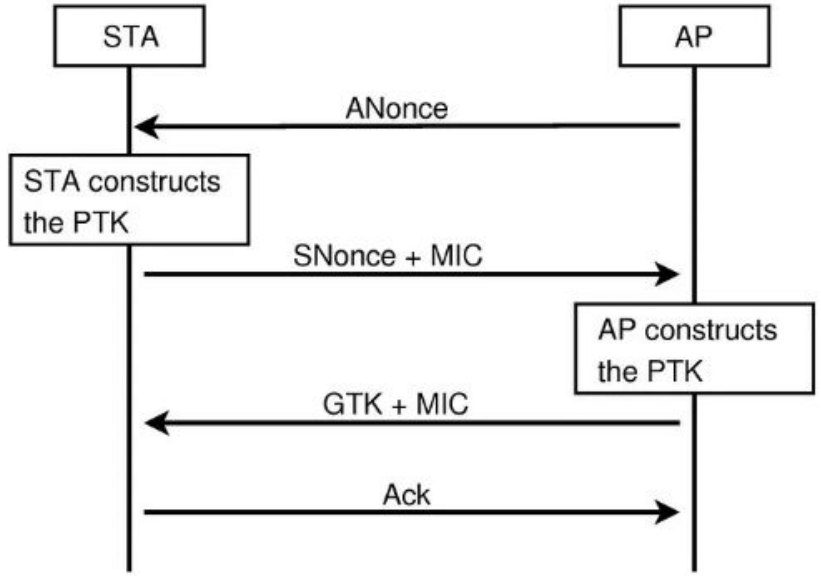
This utilizes manually configured keys in the same manner as WEP. However, the **process is more secure** because WPA incorporates the **4-Way Handshake** protocol, which ensures that both the client and the access point verify each other's identity and derive new session keys.

802.1x/EAP based Authentication (Enterprise Mode)

With WPA-Enterprise, each user or device must authenticate via a **RADIUS (Remote Authentication Dial-In User Service)** server before connecting to the network. This system enables individual credentials for each user (e.g., username/password, smart cards, or certificates) instead of relying on a shared key, as is the case with WPA-Personal. WPA-Enterprise also supports **EAP**, a framework that allows for various authentication methods to be used.

Four way Handsake

Message 1: AP sends to the client his ANONCE. Now the client has everything he needs to create the PTK because he got the ANONCE, it was the only thing that was missing for him.
Message 2: The client sends to the AP his SNONCE with a MIC, the MIC is mainly for the AP to recognize that this message is really from this client, its like a signature. Now, after the AP got the message he has everything he needs to create the PTK and that is what he does.
Message 3: The AP sends to the client the GTK because he is going to be his new client.
The client get the GTK and install it.
Message 4: The client sends to the AP that everything is OK and installed.

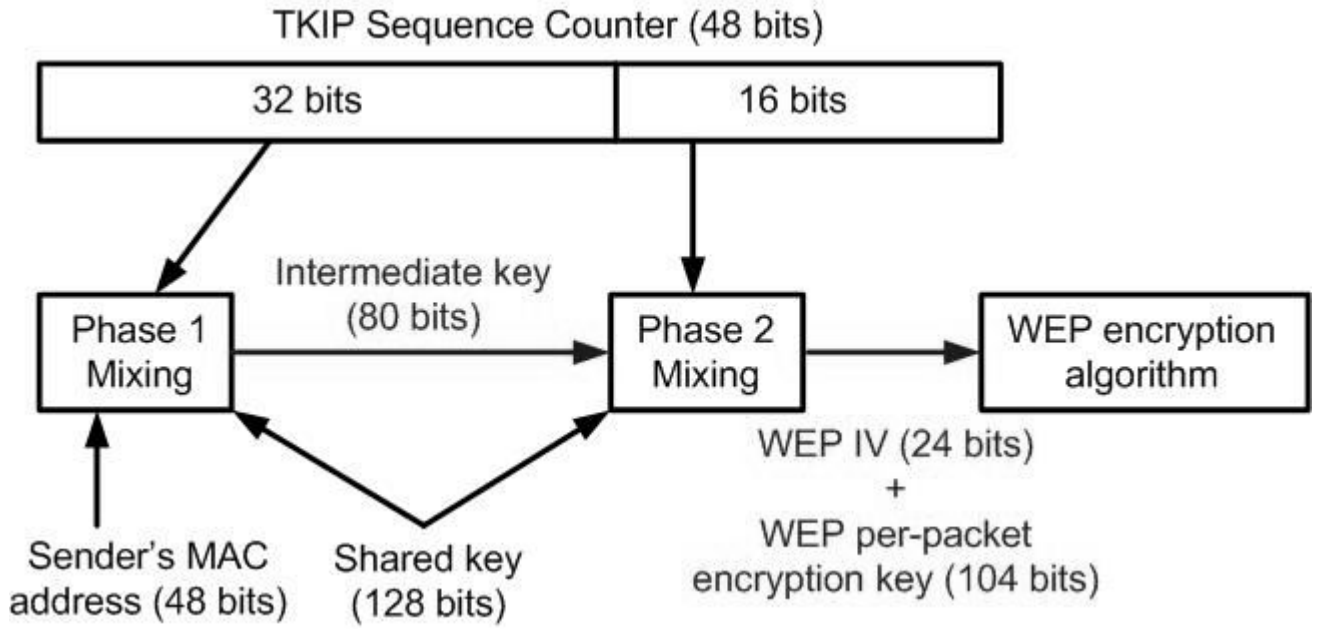


PTK - Pairwise Transit Key : The PTK is encryption for uni-cast traffic.
(PTK) = PMK + ANONCE + SNONCE + MAC(AA) + MAC(SA)
PMK- Pairwise Master Key (Pre-shared key)
GTK- Group Temporal Key: The GTK is the encryption for broadcast and multicast for the traffic between one AP to his clients. For every different AP there is a different GTK to secure the traffic in the "air" that belongs to the same network. All the clients that connect to the same AP have the same GTK.
ANONCE- is a random number that the AP has made.
SNONCE- is a random number that the client has made.
MAC(AA)- the mac address of the AP (authenticator).
MAC(SA)- the mac address of the client (supplicant).

WPA ENCRYPTION

TKIP (Temporal Key Integrity Protocol)

TKIP is an encryption protocol used in WPA. Like WEP, TKIP uses the Rivest Cipher 4 (RC4) stream encryption algorithm as its basis. However, unlike WEP, TKIP encrypts each data packet with a unique encryption key. The encryption keys are generated from the combination of shared key(temporal key obtained from PTK), sender's MAC address and packet sequence number(IV in this case).



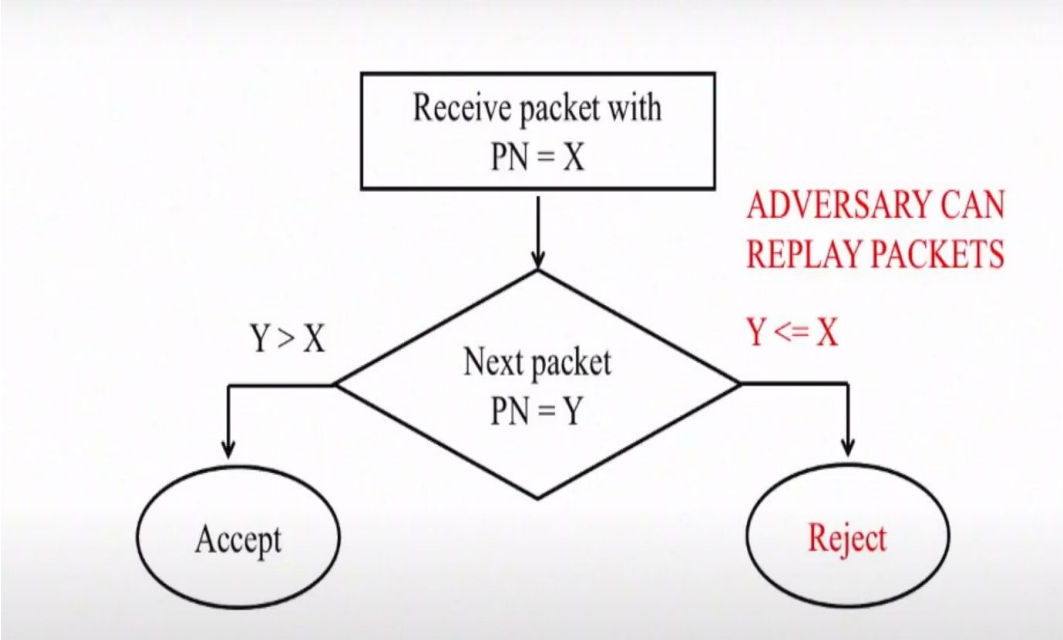
TKIP CONTINUED

- Each new packet is encrypted using a new key since the TSC stores packet sequence number. This thus helps to overcome replay attacks.
- Using MAC address in generation of keys guarantees every STATION and AP pair will generate a different set of encryption keys. This prevents key reuse problem due to cross station IV collision.
- Breaking of MIXING operations and TSC into two parts, there is no direct relationship between IV and encryption keys so if somehow the attacker gets the IV during the communication, it will not give him any other extra information

The **Message Integrity Code (MIC)** in WPA is designed to ensure the integrity of transmitted data. Its primary role is to detect any unauthorized changes to packets during transmission, thereby preventing tampering and replay attacks.
The MIC's protocol is called "Michael“. The MIC is calculated over the plaintext data of the packet (before encryption). The MIC calculation uses a secret key derived from the session's encryption keys. This ensures that only devices with the correct keys can compute a valid MIC. The calculated MIC is appended to the packet. The entire packet, including the MIC, is then encrypted. On receiver side, the message is decrypted and MIC is recalculated to ensure the data is intact or not.

Disadvantages of TKIP Encryption

- Weak encryption key as it uses RC4
- Not suited for 802.11n and newer Wi-Fi standards
- Vulnerable to various attacks such as MIC cracking and replay.

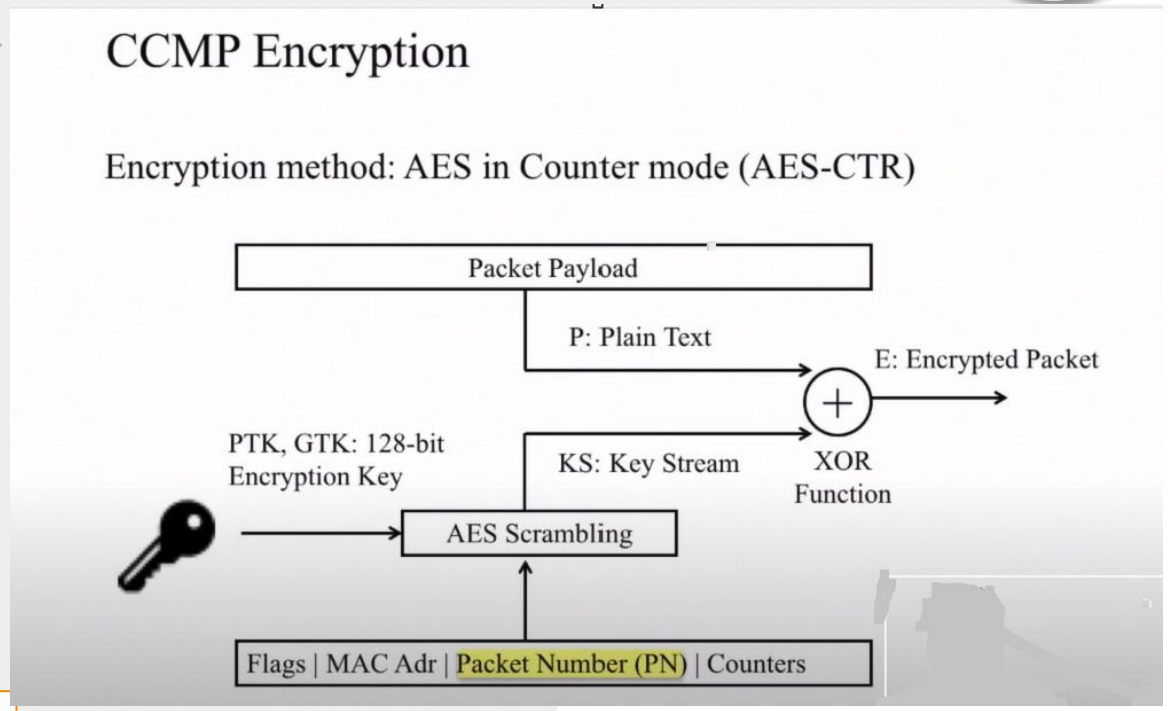


WPA2

- Was introduced in 2004 as a improvement over WPA.
- It uses RSN (Robust Security Network) for security enhancement in WPA.
- Based on 802.11i standards
- Has PSK and 802.11x/EAP based authentication
- Based on AES(Advanced Encryption Standard) and CCMP (Counter/CBC-MAC Protocol)algorithms for MIC(Message Integrity Code) and encryption.
- Uses 128 bits encryption key
- Backward compatible to WPA.

AES & CCMP ENCRYPTION

AES(Advanced Encryption Standard)



- Symmetric block cipher introduced by NIST.
- Operates on fixed size block of data 128 bits and supports size of 192, 256 bits.
- Use with CCMP combinedly.
- Counter mode encrypt the data and CBC-MAC ensures data hasn't been altered during transmission.

Suppose two packets P! and P2 are encrypted with PTK:
E1=P1+ KS1 and E2=P2+KS2,
If P1 & P2 were to use same packet number then:
KS1=KS2
In that case:
E1+E2=P1+P2 effect of encryption eliminated
If P1 is known/guessed, it is possible to decrypt P2
So, PN must be different

CCMP WORKING

CCMP(Counter Mode with Cipher Block Chaining Message Authentication Code protocol)

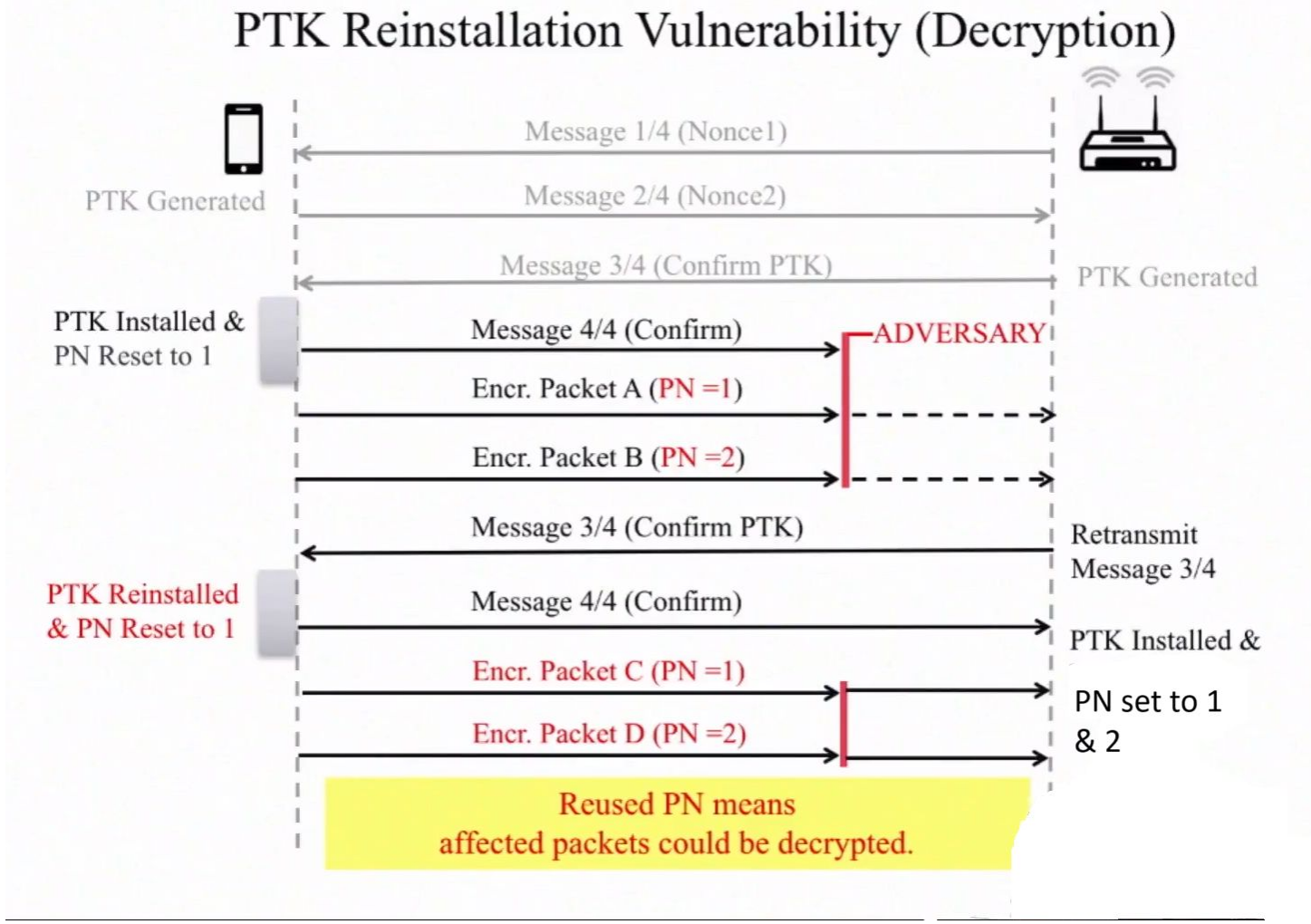
1. Initialization
   - Generates Nonce(number used once) for each packets.
   - Nonce has PN, sender address, priority value (QoS) for unique encryption.
   - Initialization Vector(IV) is derived from Nonce for encryption process.
2. Encryption (Counter Mode)
   - Plaintext is divides into 128 bits.
   - Counter is initialized for Nonce and incremented for each block.
   - AES encrypt the counter value which is XORed with plaintext to produce cipher.
3. Integrity Check (CBC-MAC)
   - MIC is calculated over entire packet using AES in CBC-MAC mode.
   - MIC is appended to the packet
4. Transmission
   - The encrypted data, MIC are sent to recipient.
5. Decryption and Validation
   - The recipient uses same AES key and Nonce to decrypt the data.
   - MIC is again calculated and compare with received MIC to verify integrity.

WPA2 Disadvantages

- Hackers can guess the password using dictionary attack (CRACK Attack).
- Users may become fatigued from regularly updating and managing strong passwords.
- Encryption and authentication can reduce network speed and performance.

WPA2 Disadvantages

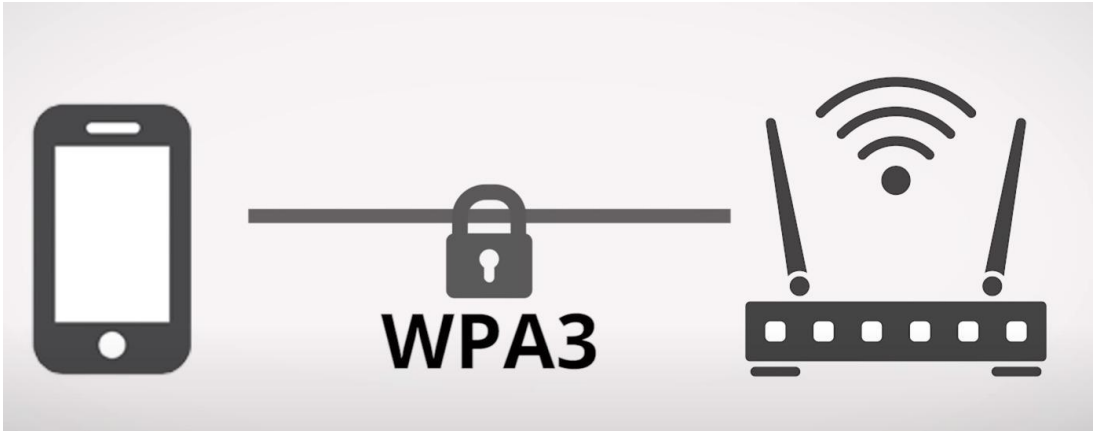
- PTK Reinstallation vulnerability



WPA3

- WPA3 (Wi-Fi Protected Access 3) is the latest generation of Wi-Fi security protocols, introduced in 2018 to enhance security for wireless networks. It addresses vulnerabilities in its predecessor, WPA2, and introduces new features to improve protection and usability. It provides cutting edge security protocols.

- WPA3 provides individualized data encryption, ensuring that data traffic between each device and the access point is encrypted separately. This prevents eavesdropping and enhances privacy, especially in public WiFi networks.



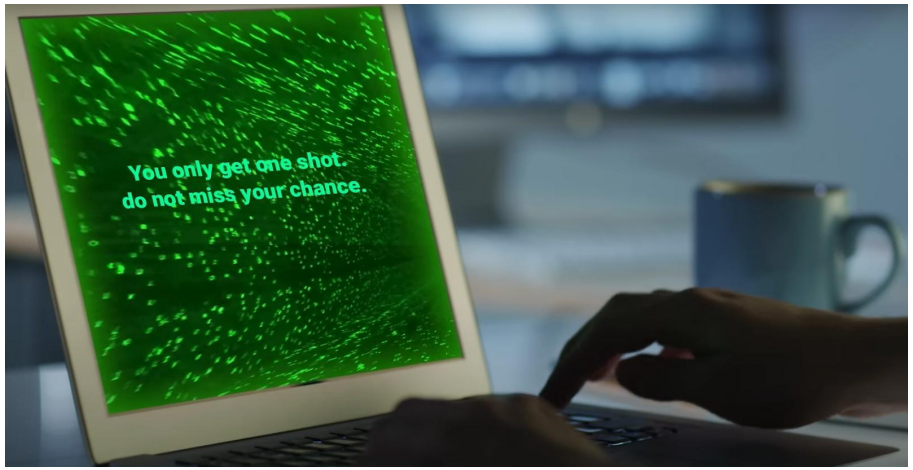
- WPA3 mandates the adoption of protected management frames, which guard against forging, and standardizes the 128 bit cryptographic suite and disallows obsolete security protocols.

- WPA3 encryption is available in two forms:

  - WPA3-Personal: This replaces the 4-way handshake with Simultaneous Authentication of Equals (SAE) and which is defined in the IEEE 802.11s standard. SAE was initially defined for mesh networks, but is now scaling to infrastructure wireless networks.

  - WPA3-Enterprise: This integrates a back-end authentication infrastructure, such as with a RADIUS server. Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve are used to a strong authentication.

- WPA3 provides almost seamless protection against brute-force attacks for network passwords. SAE replaces the pre-shared key (PSK) method used in WPA2, providing a more secure way to authenticate wireless devices. SAE resists offline brute-force attacks and makes it significantly harder for attackers to guess passwords. The protection only allows for one change to crack a password.



- Along with these changes, WPA-3 brings the integration of QR codes to gain the network connection details.

Features

- Improved Security for Passwords

  Simultaneous Authentication of Equals (SAE): Replaces the Pre-Shared Key (PSK) authentication in WPA2. SAE provides stronger protection against password-guessing attacks, even if the password is weak.

- Public WiFi Network Security

  Encrypts data between the device and the router, providing unique encryption for each user on the same network. This enhances privacy, especially on public Wi-Fi networks.

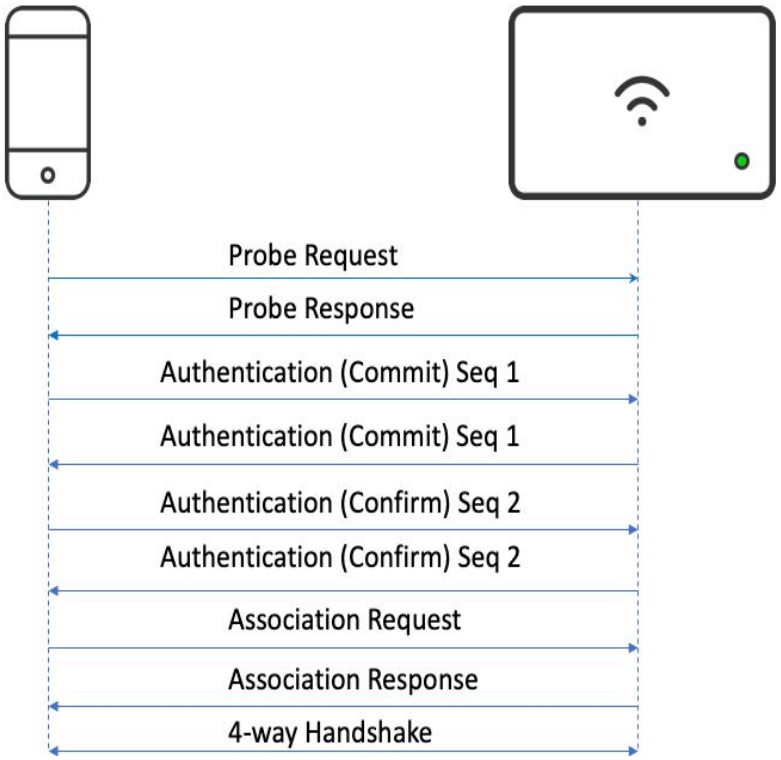
- Forward Secrecy

  Even if the password or shared key is compromised in the future, past session keys and communications remain secure.

- Enhanced Security for IoT Devices

  WPA3's Easy Connect simplifies the process of securely connecting IoT devices that lack user interfaces, like smart thermostats or cameras.

SAE



1. Probe Request
    - Regular request to AP after beacon.
2. Probe Response
    - Regular response to STA.
3. Authentication (Commit) from STA to AP
    - This packet is an 802.11 authentication frame.
    - Commit will include SAE authentication Seq Number 1 with a scalar and an element not related to the password to be used.
    - This is used to generate the PMK on the STA.
4. Authentication (Commit) from AP to STA
    - This packet is an 802.11 authentication frame.
    - Commit will include SAE authentication Seq Number 1 with a scalar and an element not related to the password to be used.
    - This is used to generate the PMK on the AP.
5. Authentication (Confirm) from STA to AP
    - This packet is an 802.11 authentication frame.
    - Confirm includes Seq Number 2 with confirm message with key generated for AP to validate.
6. Authentication (Confirm) from AP to STA
    - This packet is an 802.11 authentication frame.
    - Confirm includes Seq Number 2 with confirm message with key generated letting STA know the key is correct or rejecting the authentication.
7. Regular Association Request
8. Regular Association Response
9. 4-way handshake utilizing PMK generated with SAE method. After this step regular data can be transmitted

Dragonfly handshake

• In WPA3, the Dragonfly handshake is used during the initial connection to establish a secure shared key between the client and the access point (AP). The Dragonfly handshake is essentially a SPEKE (Simple Password Exponential Key Exchange) protocol.

Steps in Dragonfly Handshake (Simplified):

• Password Element Derivation:

Both the client and the AP derive a "password element" (PE) from the shared password. This process uses elliptic curve or finite field cryptography, ensuring the password is never directly transmitted.

• Commit Exchange:

Both parties generate random values and send commit messages to each other. These messages include their public keys but do not reveal the password.

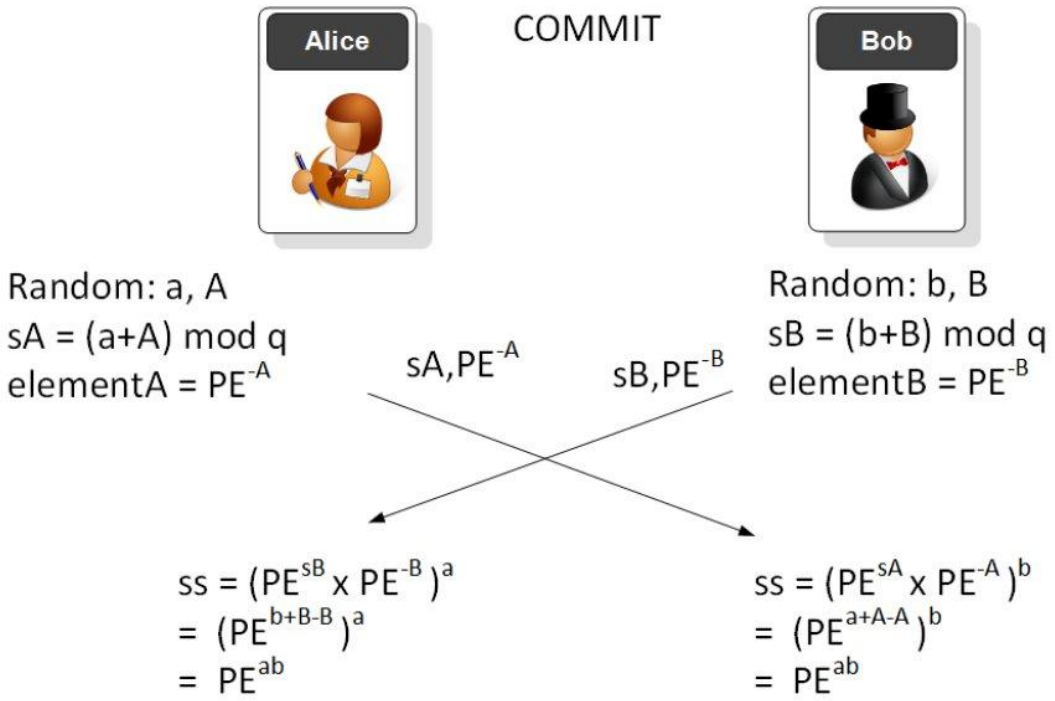
• Confirm Exchange:

Both parties use the received commit messages to calculate the shared secret and verify its correctness by exchanging confirm messages. These messages confirm that both parties have derived the same key.

• Session Key Establishment:

After successful confirmation, both the client and AP use the shared key to encrypt subsequent communications.

In the commit phase, Alice (the client) generates two random values (a,A), then computes a scalar value (a+A). The value that Alice will pass is the PE (Password Equivalent—such as hashed value of the password that Bob and Alice know) raised to the power of -A. The operations are done with (mod q) and where q is a large prime number. Bob does the same, and then they exchange values. In the end they will have the same shared commit key (PE^{ab}). The password has been used to validate Bob and Alice, and they will only have the shared shared commit value if they both have the same password. The intruder cannot determine either the original password or the final shared value.



While WPA3 offers significant improvements over its predecessor, it is not without shortcomings. Here are some of the key issues and challenges associated with WPA3:

- Transition Mode Vulnerability
- Dragonblood Vulnerabilities
- Limited Device Support
- Cost of Upgrades

WPA3 is not unaffected by threats and has several security flaws. But, experts still agree that it is the most secure protocol

THANK YOU!