### Q6)The Role of the Pairwise Master Key (PMK) in the 4-Way Handshake

The **Pairwise Master Key (PMK)** is a critical component in Wi-Fi security, particularly in the **4-way handshake** used by WPA2 and WPA3.

**1. What is the PMK?**

* The PMK is a **256-bit key** derived during the authentication process.
* In **WPA2-Personal (PSK)**, the PMK is generated from:
* The Wi-Fi **pre-shared key (password)**.
* The **SSID (network name)**.
* A **hashing algorithm (PBKDF2 with SHA-1)**.
* In **WPA2/WPA3-Enterprise (802.1X)**, the PMK is created by the RADIUS server and sent to the access point (AP).

**2. Role of the PMK in the 4-Way Handshake**

The **4-way handshake** is used to:

* **Authenticate** the client and access point (AP).
* **Derive fresh encryption keys** for the session (to prevent replay attacks).
* **Confirm mutual possession of the PMK** without transmitting it directly.

**Step-by-Step Role of the PMK:**

1. **PMK Exists Before the Handshake**
   * The AP and client already have the PMK (pre-shared or from 802.1X authentication).
2. **Handshake Messages (4 Steps):**
   * **Message 1 (AP → Client):**
     + AP sends a **nonce (ANonce)** to the client.
     + Client uses **PMK + ANonce + SNonce (client nonce)** to compute the **Pairwise Transient Key (PTK)**.
   * **Message 2 (Client → AP):**
     + Client sends its **SNonce** and a **MIC (Message Integrity Code)** to prove it knows the PMK.
   * **Message 3 (AP → Client):**
     + AP verifies the MIC, then sends the **Group Temporal Key (GTK)** for multicast traffic.
   * **Message 4 (Client → AP):**
     + Client confirms installation of keys, completing the handshake.
3. **Key Derivation:**
   * The **PTK** (used for encrypting unicast traffic) is derived from:

**3. Why the PMK is Essential**

* **Never Transmitted Over Air:**
  + The PMK itself is **never sent** during the handshake, preventing eavesdropping.
  + Only **nonces and MICs** are exchanged to prove PMK knowledge.
* **Session-Specific Keys:**
  + Each session generates a unique **PTK**, ensuring **forward secrecy** (compromising one session doesn’t affect others).
* **KRACK Attack Vulnerability (WPA2):**
* The 2017 KRACK attack exploited **handshake replay** to force nonce reuse, allowing PTK recovery.
* **WPA3 fixes this** with **Simultaneous Authentication of Equals (SAE)**.

**4. PMK in WPA3 (Improvements)**

* **WPA3-Personal (SAE):**
  + Replaces PSK with **Dragonfly Key Exchange (SAE)**, making PMK derivation resistant to offline dictionary attacks.
* **WPA3-Enterprise:**
  + Uses **192-bit cryptographic suites** for stronger PMK security.

|  |  |
| --- | --- |
| Function | Details |
| Pre-Shared Secret | Derived from Wi-Fi password (PSK) or RADIUS server (Enterprise). |
| PTK/GTK Derivation | Generates session-specific encryption keys via the 4-way handshake. |
| Authentication Proof | Client/AP prove PMK ownership via MICs without transmitting the PMK. |
| Security Foundation | Critical for WPA2/WPA3; weaknesses in PMK derivation (e.g., weak passwords) weaken the entire system. |