**WiFi Training Program - Module 6 Assignment Answers**

**Q1.**

Wi-Fi security is built upon three foundational pillars:

* **Authentication**: This is the process of verifying the identity of a device or user attempting to connect to a wireless network. Only authorized users should be able to connect. Examples include pre-shared keys (PSK), WPA2-Enterprise with RADIUS, and 802.1X with EAP.
* **Encryption**: Once authenticated, data transmitted between the client and access point needs to be protected from eavesdropping. Encryption ensures data confidentiality. WPA2 uses AES-based CCMP, while WPA3 uses AES-GCMP for stronger encryption.
* **Integrity**: Data integrity ensures that information is not altered or tampered with during transmission. Techniques like Message Integrity Code (MIC) are used to detect any changes in the data.

**Q2.**

* **Authentication** is concerned with *who is allowed to connect*. It verifies the identity of users or devices. Without successful authentication, access to the network is denied.
* **Encryption** is focused on *what is being transmitted*. It secures data by transforming it into an unreadable format for unauthorized parties, ensuring confidentiality.

Authentication establishes trust, and encryption ensures privacy and security of data

**Q3.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Protocol** | **Introduced** | **Encryption Method** | **Key Management** | **Security Level** |
| **WEP** | 1997 | RC4 (static) | Weak (manual key entry) | Poor - easily broken |
| **WPA** | 2003 | TKIP (RC4-based) | Dynamic key generation | Moderate - patch over WEP |
| **WPA2** | 2004 | AES-CCMP | Robust key management | Strong - industry standard for years |
| **WPA3** | 2018 | AES-GCMP + SAE | Simultaneous Authentication of Equals | Very strong - resistant to brute force attacks |

WPA2 was a complete redesign using AES encryption, and WPA3 improves security further by preventing offline password-guessing and providing forward secrecy.

**Q4.**

WEP is insecure due to multiple vulnerabilities:

* Uses the outdated RC4 encryption algorithm with static keys.
* Initialization Vector (IV) is too short (24-bit), leading to collisions.
* No effective key management or rotation.
* Susceptible to replay attacks and IV reuse.

Tools like Aircrack-ng can crack WEP in minutes, making it obsolete and unsafe.

**Q5.**

WPA2 was introduced to:

* Replace WPA (which was a temporary fix using TKIP over RC4).
* Provide a more robust security mechanism with **AES-CCMP**.
* Comply with modern security standards.
* Enable enterprise-level authentication with 802.1X and RADIUS.

WPA2 became mandatory for Wi-Fi Certified devices in 2006.

**Q6.**

The PMK is a 256-bit key derived from:

* A pre-shared key (in WPA-PSK mode), or
* An EAP method in WPA2-Enterprise (after successful 802.1X authentication).

In the 4-way handshake:

* PMK is used to derive the **Pairwise Transient Key (PTK)**.
* PTK is then used for encrypting data and ensuring its integrity using subkeys (KCK, KEK, TK).
* PMK ensures both sides can independently generate the same PTK without sending sensitive data.

**Q7.**

The 4-way handshake verifies possession of the PMK by both parties:

1. **Message 1**: AP sends a nonce (ANonce) to the client.
2. **Message 2**: Client uses ANonce + SNonce + PMK to derive PTK and sends SNonce and MIC.
3. **Message 3**: AP verifies MIC using its own PTK derivation, confirms match, and sends GTK + MIC.
4. **Message 4**: Client verifies AP's MIC and completes the handshake.

Any mismatch results in handshake failure, ensuring both parties possess the correct PMK.

**Q8.**

* The client will derive an incorrect PMK and PTK.
* MIC values computed using the wrong keys will not match.
* The access point will reject the handshake due to MIC validation failure.
* Result: The connection will fail, and the client will not be authenticated or connected.

**Q9.**

802.1X provides **port-based network access control**, solving:

* Centralized user authentication using a RADIUS server.
* Avoidance of shared passwords in large networks.
* Dynamic generation of unique encryption keys per session.
* Prevention of unauthorized access even if a user knows the SSID.

It's essential for **enterprise-level network security**.

**Q10.**

802.1X enhances security by:

* Using **EAP (Extensible Authentication Protocol)** for flexible authentication methods (certificates, tokens, etc.).
* Issuing a **unique PMK per session**, reducing the chance of key reuse.
* Preventing unauthorized access to the LAN until authentication is successful.
* Supporting mutual authentication: both client and server verify each other.
* Enabling per-user policies and access control.

Overall, it eliminates static password vulnerabilities and strengthens access security in wireless environments.