Wifi Training Assignment 6

- Yuvan Shankar G

Problem1:

Pillars of Wi-Fi Security

- Authentication: Verifies identity of users or devices.
- Encryption: Protects data from eavesdropping.
- Integrity: Ensures data isn't tampered with.
- Key Management: Manages cryptographic keys securely.

Problem2:

Difference Between Authentication and Encryption

- Authentication: Confirms user/device identity before access.
- Encryption: Secures data transmitted over the network.
- Authentication happens first; encryption ensures secure data exchange afterward.

Problem3:

Differences Between WEP, WPA, WPA2, and WPA3

- WEP: Weak RC4 encryption, static keys, easily cracked.
- WPA: Improved over WEP with TKIP, still used RC4.
- WPA2: Introduced AES-CCMP, stronger encryption, 4-way handshake.
- WPA3: Uses SAE instead of PSK, provides forward secrecy, more secure in public networks.

Problem4:

WEP is Insecure Compared to WPA2/WPA3

- WEP uses short, predictable IVs that repeat.
- Weak RC4 algorithm and static keys.
- Can be broken in minutes using basic tools.
- Offers almost no real security in modern environments.

Problem5:

Reason for Introduction of WPA2

- WPA2 was introduced to replace insecure WEP and flawed WPA.
- It uses AES-CCMP for robust encryption.
- Implements a secure 4-way handshake and key management.
- Became the mandatory standard for Wi-Fi security.

Problem6:

Role of Pairwise Master Key (PMK)

- PMK is derived from the passphrase (PSK) or 802.1X authentication.
- It is not used directly but to derive PTK.
- PMK ensures secure foundation for session encryption.
- Both AP and client must know the same PMK to establish a secure connection.

Problem7:

Mutual Authentication via 4-Way Handshake

- AP sends ANonce to client.
- Client sends SNonce and computes PTK using PMK, ANonce, SNonce, and MAC addresses.
- AP uses same values to derive matching PTK.
- If PTKs match, both parties confirm via MIC.
- Ensures mutual possession of correct PMK without transmitting it.

Problem8:

Result of Wrong Passphrase in 4-Way Handshake

- Incorrect passphrase → incorrect PMK → incorrect PTK.
- MIC verification fails during handshake.
- AP rejects the connection.
- Client will not be able to join the network.

Problem9:

Problem Solved by 802.1X

- 802.1X controls access before granting network connectivity.
- Prevents unauthorized devices from joining.
- Supports centralized authentication via RADIUS.
- Eliminates reliance on shared keys in enterprise environments.

Problem10:

How 802.1X Enhances Wireless Security

- Uses EAP methods for flexible, secure authentication.
- Generates dynamic encryption keys per session.
- Integrates with RADIUS for per-user access control.
- Prevents unauthorized access and enhances data confidentiality.