Name: Aswath S

College: Vellore Institute of Technology, Vellore

Reg.No: 21BEC2188

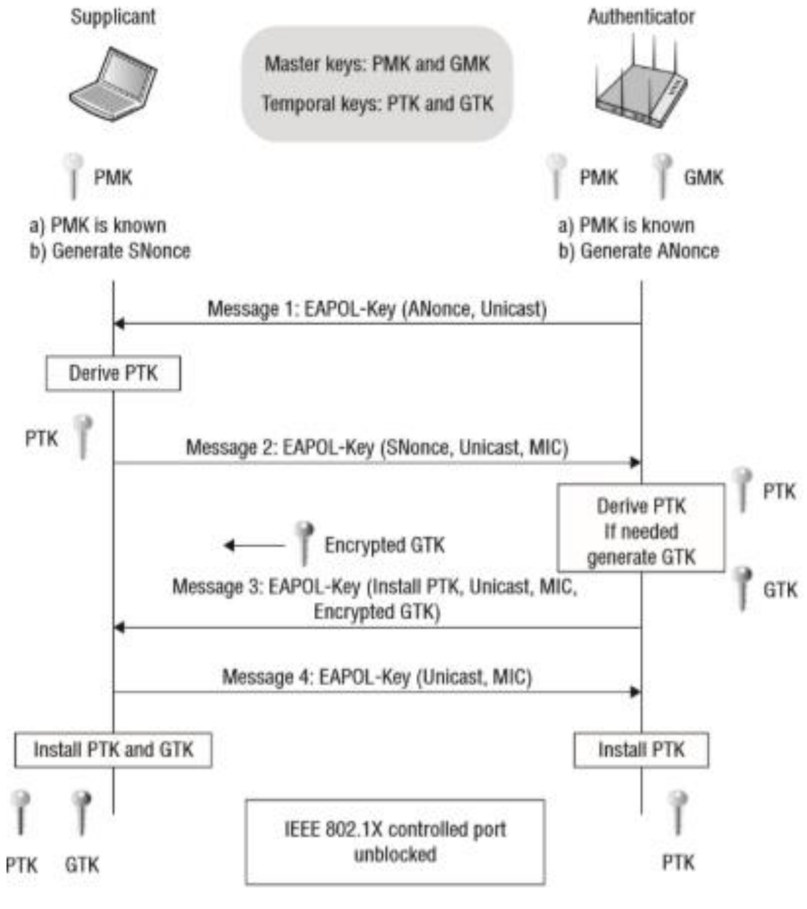
Wi-Fi Training Program 2025

Module 4

Question 6:

Explain each step involved in EAPOL 4-way handshake and the purpose of each keys derived from the process.

Solution:


Supplicant
Master keys: PMK and GMK
Temporal keys: PTK and GTK
Authenticator
PMK
PMK
GMK
a) PMK is known
b) Generate SNonce
a) PMK is known
b) Generate ANonce
Message 1: EAPOL-Key (ANonce, Unicast)
Derive PTK
PTK
Message 2: EAPOL-Key (SNonce, Unicast, MIC)
Derive PTK
If needed
generate GTK
PTK
Encrypted GTK
GTK
Message 3: EAPOL-Key (Install PTK, Unicast, MIC, Encrypted GTK)
Message 4: EAPOL-Key (Unicast, MIC)
Install PTK and GTK
Install PTK
PTK
GTK
IEEE 802.1X controlled port unblocked
PTK

- **PMK (Pairwise Master Key):** Derived from the user's password (pre-shared key) or authentication (802.1X). It is shared between the supplicant and authenticator.

- **GMK (Group Master Key):** Held only by the authenticator; used to derive GTK.

- **PTK (Pairwise Transient Key):** Derived from PMK, used for encrypting unicast traffic.

- **GTK (Group Temporal Key):** Used to encrypt broadcast/multicast traffic.

- **SNonce/ANonce:** Random numbers generated by supplicant/authenticator for PTK derivation.

Steps in the 4-Way Handshake:

Message 1: Authenticator → Supplicant

- Authenticator sends **ANonce** to the supplicant.
- Purpose: Begin handshake and share a random number (ANonce).
- Supplicant already knows PMK and now receives ANonce.

Supplicant: Derive PTK

- Supplicant generates **SNonce**.
- Uses PMK, SNonce, ANonce, and MAC addresses to derive the **PTK**.
- PTK is split into multiple keys:
  - **KCK (Key Confirmation Key)** – for message integrity
  - **KEK (Key Encryption Key)** – for encrypting the GTK
  - **TK (Temporal Key)** – for encrypting data frames

Message 2: Supplicant → Authenticator

- Sends **SNonce** and a **Message Integrity Code (MIC)** using PTK.
- Authenticator now has both ANonce and SNonce, and knows PMK.
- It uses them to **derive the same PTK**.

Authenticator: Derive PTK and Generate GTK

- Authenticator derives PTK from PMK, ANonce, SNonce, and MAC addresses.
- If GTK needs to be updated, it is encrypted using KEK.

Message 3: Authenticator → Supplicant

- Sends the encrypted **GTK**, MIC, and a confirmation to install PTK.
- Purpose: Deliver GTK securely and confirm PTK installation.

Message 4: Supplicant → Authenticator

- Acknowledges the successful installation of PTK and GTK using MIC.
- Purpose: Final confirmation that keys are installed and ready.