HACK WIFI

From Connection to Compromise:
The PMKID Attack

NATIONAL CYBERSECURITY
STUDENT ASSOCIATION

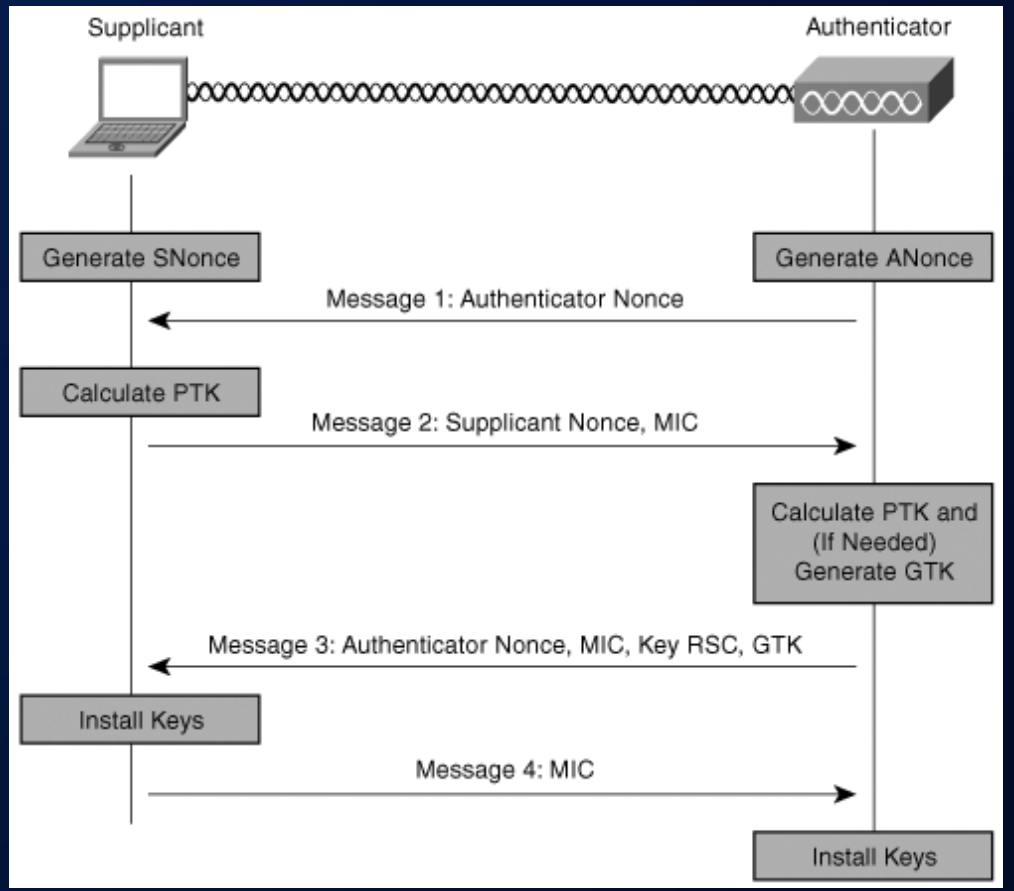
Four-Way Handshake

The four-way handshake is a security protocol used in WPA/WPA2 WiFi networks to validate that both the client and the Access Point (AP) each have the proper credentials.

During the handshake, unique encryption keys are derived and exchanged, ensuring secure communication between the client and the AP.

To exploit the handshake, one only needs to capture the PMKID (from the first handshake message) and does not require a client to be actively connecting.

Once the PMKID is captured, it can be used offline to derive the PMK (and thus the PSK) by brute-forcing its values against the known PMKID.



Four-way handshake

Client (PC)

Authentication request frame

Authentication response frame

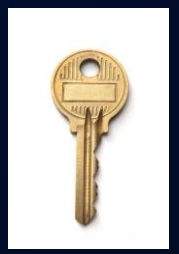
Association request frame

Association response frame

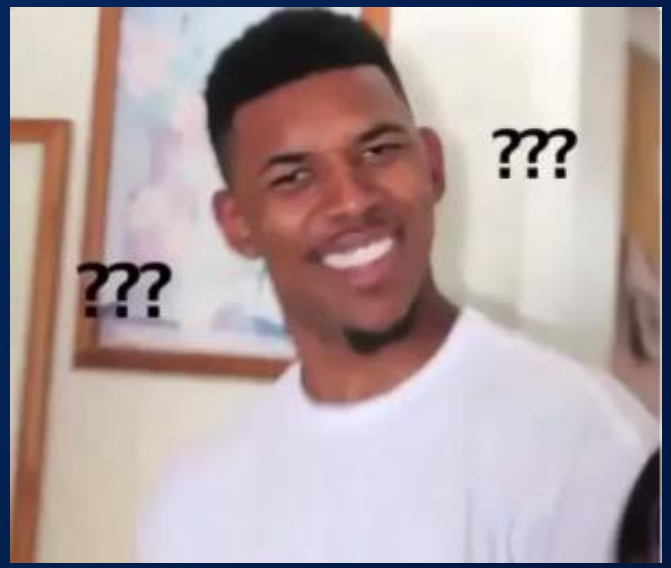
Access point (Router)

PMK

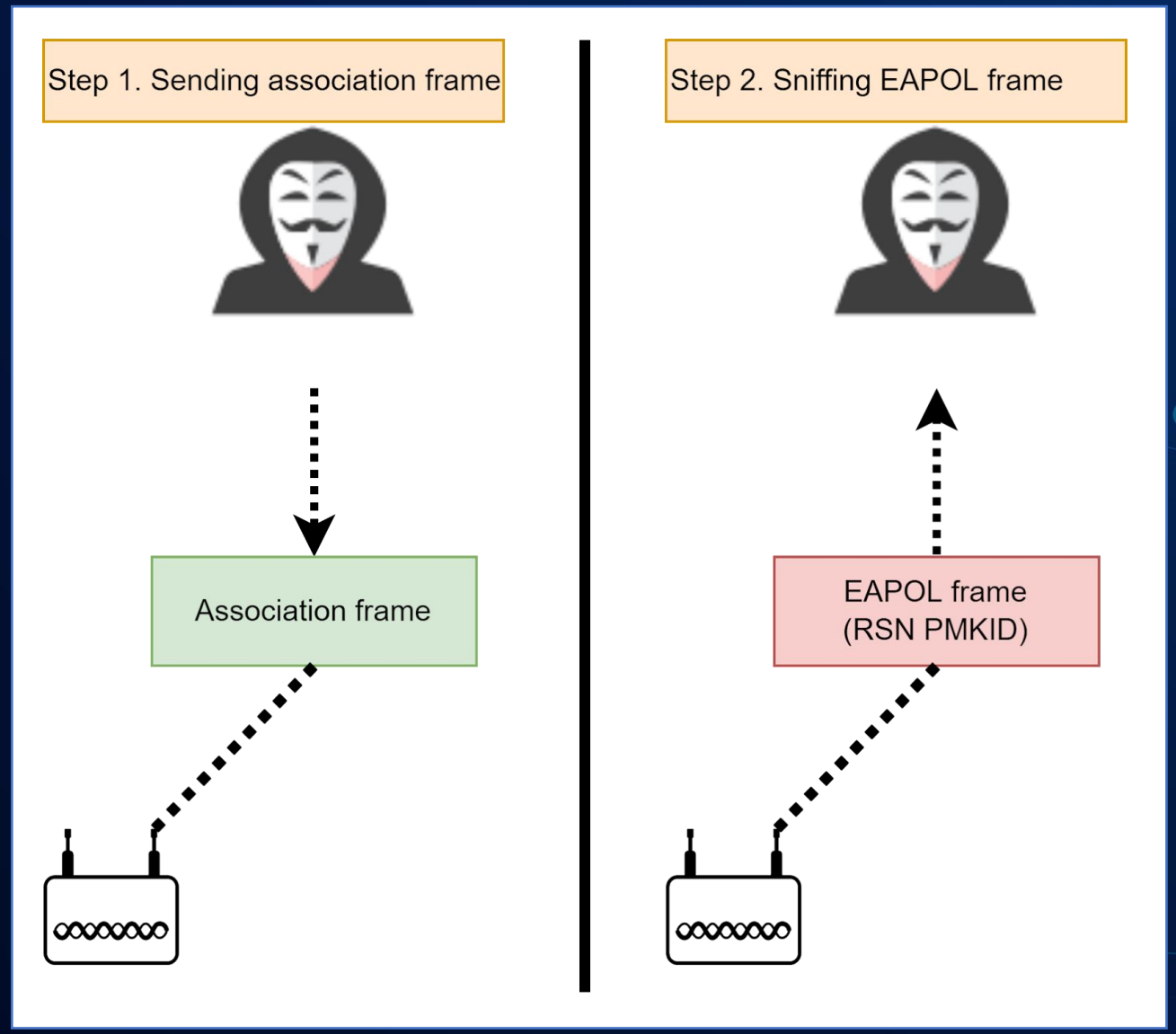
PMK



Four-way handshake

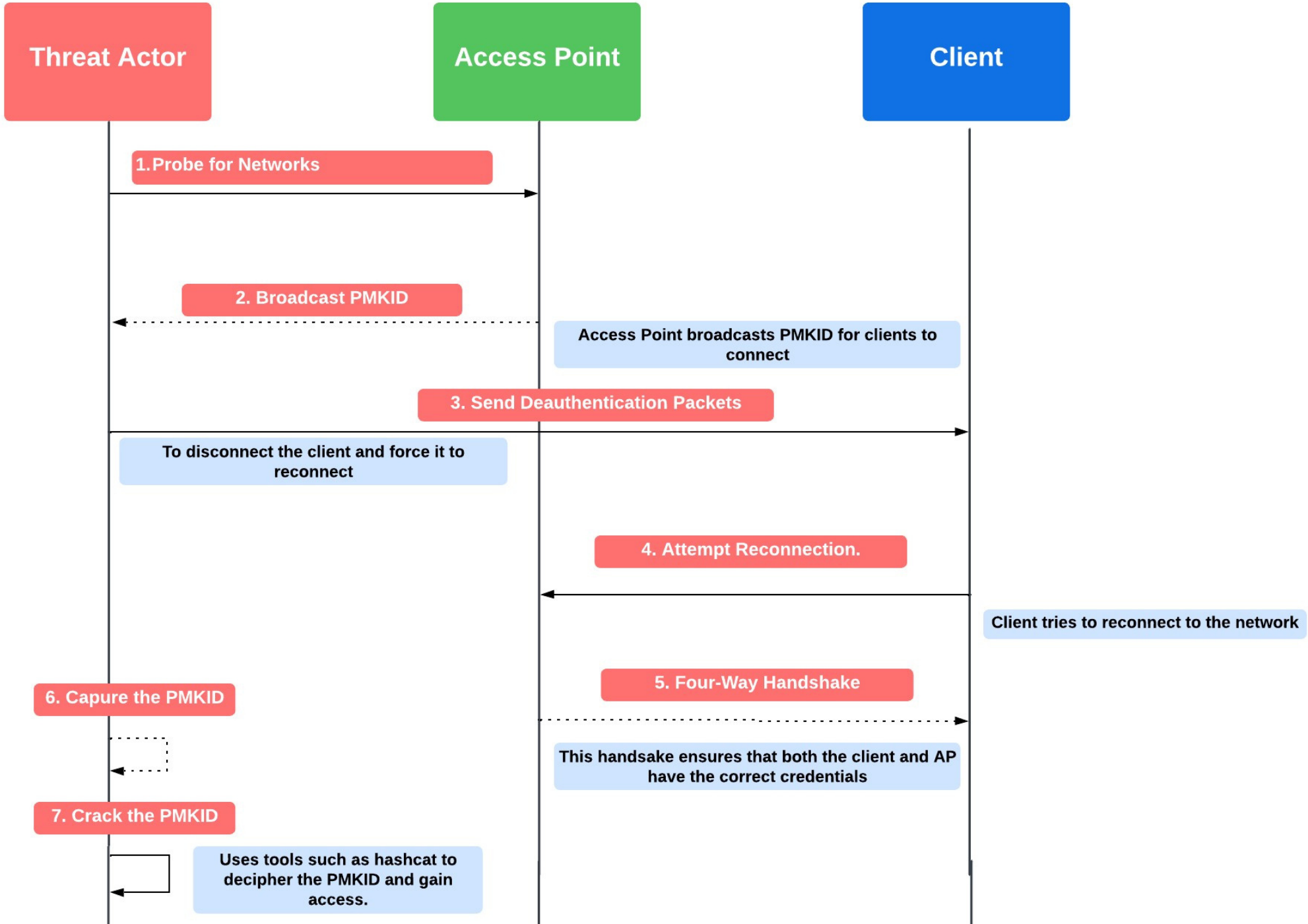


Cached PMKID


Step 1. Sending association frame
Association frame
Step 2. Sniffing EAPOL frame
EAPOL frame
(RSN PMKID)

PMKID Attack Path

1. Probe for Networks
2. Observe AP Broadcasting the PMKID
3. Capture the PMKID
4. Crack the PMKID!


Threat Actor
Access Point
Client
1.Probe for Networks
2. Broadcast PMKID
Access Point broadcasts PMKID for clients to connect
3. Send Deauthentication Packets
To disconnect the client and force it to reconnect
4. Attempt Reconnection.
Client tries to reconnect to the network
5. Four-Way Handshake
This handsake ensures that both the client and AP have the correct credentials
6. Capure the PMKID
7. Crack the PMKID
Uses tools such as hashcat to decipher the PMKID and gain access.