Securing Wireless LANs: Part 4

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- J. Kurose, K. Ross, "*Computer Networking: A Top Down Approach*", Sixth Edition, Pearson Education, 2013
- J. Edney, W.A. Arbaugh, "*Real 802.11 Security: Wi-Fi Protected Access and 802.11i*", Pearson Education, 2004.
- B.L. Menezes, R. Kumar, "*Cryptography, Network Security, and Cyber Laws*", Cengage Learning India Pvt.Ltd., 2018

Key Derivation

- Recall: station and AP agree upon Pairwise Master Key (PMK) in one of two ways:
  - station and authentication server may agree on it during their mutual authentication; latter then conveys it to AP
  - if Pre-Shared Key (PSK) mode is used, then PMK is a function of the PSK, which is manually installed in AP and station
- The 256-bit PMK is used to derive a 384-bit Pairwise Transient Key (PTK)
  - PTK is a pseudo-random function of the PMK, two nonces chosen by the AP and the station and their MAC addresses

Key Derivation (contd.)

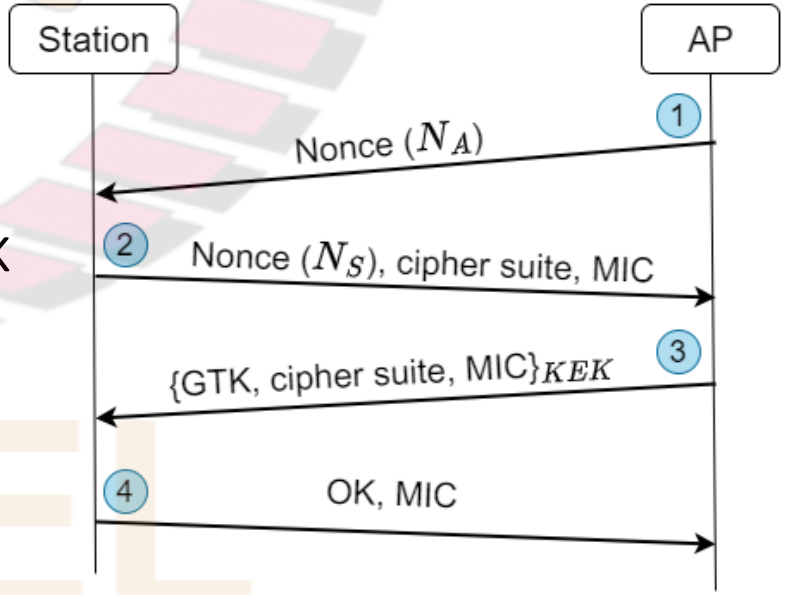
- Recall: the 256-bit PMK is used to derive a 384-bit Pairwise Transient Key (PTK)
- Three 128-bit chunks are extracted from the 384-bit PTK:
  - ❑Temporal Key (TK) used for encryption and message integrity protection of data between the AP and the station
  - ❑Key Confirmation Key (KCK) used to integrity-protect some of the messages in the four-way handshake (details later)
    - Integrity protection provided by a MAC computed as a function of the message and the KCK
  - ❑Key Encryption Key (KEK) used to encrypt the message containing the group key in the four-way handshake (details later)

Four-Way Handshake

- Four-way handshake performed between station and AP after they have agreed upon PMK
- Goals:
  - ❑to derive the PTK from the PMK
  - ❑to verify the cipher suites to be used in the subsequent data communication
    - o recall: AP and STA select the cipher suite during the first phase (discovery) of their mutual authentication
  - ❑to communicate the group key from AP to station

Four-Way Handshake (contd.)

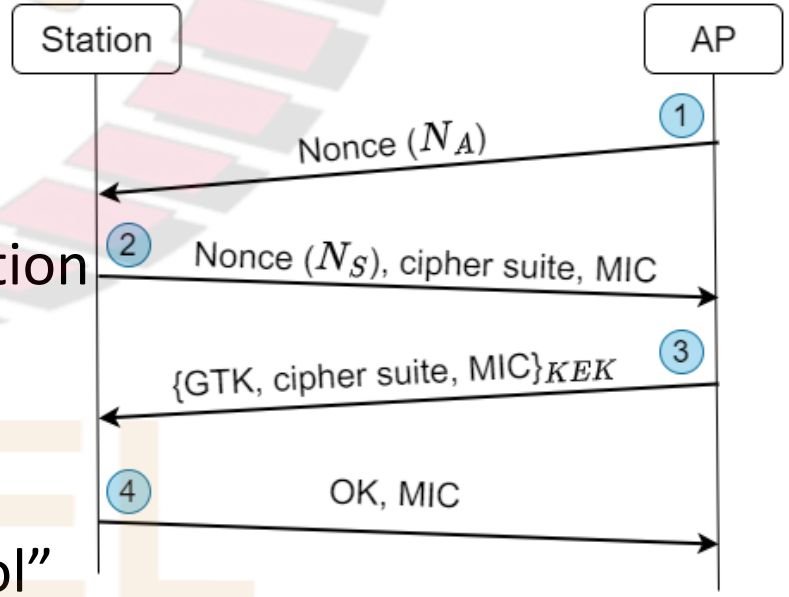
1) AP sends a nonce, N_A, to station
2) Station chooses a nonce, N_S
   - Station computes PTK using:
     a) $PTK = prf(PMK, N_A, N_S, MAC_A, MAC_S)$,
     - where *prf* is a pseudo-random function and MAC_A and MAC_S are the MAC addresses of the AP and station
   - Reason for using the two nonces:
     - to defend against replay attacks
   - As stated earlier, the TK, KCK and KEK are extracted from the PTK
   - Station sends its nonce together with its choice of cipher suite to AP
     - KCK used to compute a Message Integrity Check (MIC)
     - MIC helps in defending against a possible man-in-the-middle attack, intended to remove the strong algorithms from the cipher suite, thus forcing AP to choose weak ones
   - On receiving message 2, AP computes PTK using expression in a), and extracts TK, KCK and KEK from it
   - Also, AP verifies the integrity of message 2 using KCK



Four-Way Handshake (contd.)

3) Message 3 from AP to station contains the current Group Transient Key (GTK)
   - ❑ GTK is the key used by the AP and all stations to integrity protect (and optionally encrypt) all broadcast messages
   - ❑ Message 3 also contains the cipher suite chosen by AP
   - ❑ Message 3 is encrypted using KEK and integrity-protected using KCK
4) Message 4 is an acknowledgement from the station that it has received the previous messages without error

- After the above four-way handshake is completed, all messages are integrity-protected and encrypted using the Temporal Key (TK)
- *Note*: Recall that "MAC" is an abbreviation for "Message Authentication Code". However, in 802.11 standard, the term "MIC" used instead of "MAC" to avoid confusion with "Medium Access Control"



Pairwise Master Key and Temporal Key

- Recall:
  - PMK and exchange of two nonces, one in each direction, are used to create Temporal Key (and also KCK and KEK)
  - Temporal Key used for encryption and message integrity
- Why is PMK itself not used for encryption and message integrity?
- Recall: it is insecure to use long-term keys used for authentication, for encryption and message integrity within each session
  - secure to generate a session key, which is different for each session
- Temporal Key is a session key
  - before each data exchange session, new Temporal Key is generated, and it is discarded at the end of the session
- Recall:
  - Master Secret (Master Key) generated after TLS authentication is a function of two nonces; hence different for different sessions
  - So if EAP-TLS used, then PMK is different for different sessions
- Then why is Temporal Key derived from PMK and two nonces?
  - since for authentication, techniques other than EAP-TLS may be used, under which PMK is same for each session
  - e.g., PSK or EAP with some protocol other than TLS may be used

RADIUS and Diameter

- There are different types of authentication servers
- Remote Access Dial-In User Service (RADIUS) is a popular standard specified by the Internet Engineering Task Force (IETF)
- RADIUS defines the following:
  1) a set of functionalities, which a RADIUS authentication server should have
  2) a protocol that allows other devices (e.g., APs) to communicate with a RADIUS authentication server
- RADIUS authentication servers can be used in:
  - the context of Wi-Fi (802.11i) and
  - more generally, in contexts where users use some network service via devices called *network access servers*
  - e.g., dial-up, cloud computing
  - Note: in case of Wi-Fi, users are those that connect wirelessly using a laptop, mobile, etc., and APs are network access servers
- Many practical corporate networks use RADIUS servers
- Diameter is another standard for an authentication server; it is an improved version of RADIUS