Securing Wireless LANs: Part 3

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

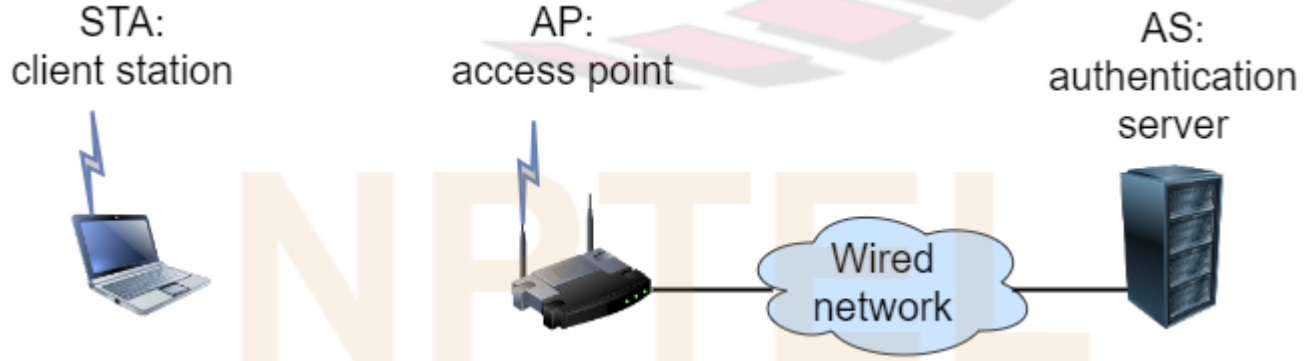
WPA and 802.11i

802.11i

- 802.11i also known as WPA2 (Wi-Fi Protected Access 2)
  - ❑became available in 2004
- WPA became available in 2003
  - ❑was intended as an intermediate measure in anticipation of the more secure and complex WPA2
  - ❑sometimes referred to as the draft 802.11i standard
- 802.11i provides better security than WEP:
  - ❑stronger encryption than in WEP
  - ❑mutual authentication (*i.e.*, mobile device and AP authenticate each other)
  - ❑a key distribution mechanism
  - ❑stronger message integrity

Authentication Server

- In addition to mobile device and AP, 802.11i defines an "*authentication server*", which has a secure connection with the AP
  - ❑ *e.g.*, a server containing a username and password database
- *E.g.*: a corporate or university campus may have an authentication server connected to its LAN; communicates over LAN with all the APs in campus
- During authentication, AP acts as a relay, forwarding messages from authentication server to mobile device and vice versa
- Advantages of separating authentication server from AP:
  - ❑ AP complexity and costs can be kept low
  - ❑ the sensitive information and decisions regarding authentication are confined to only one entity (the authentication server), instead of being replicated at each AP

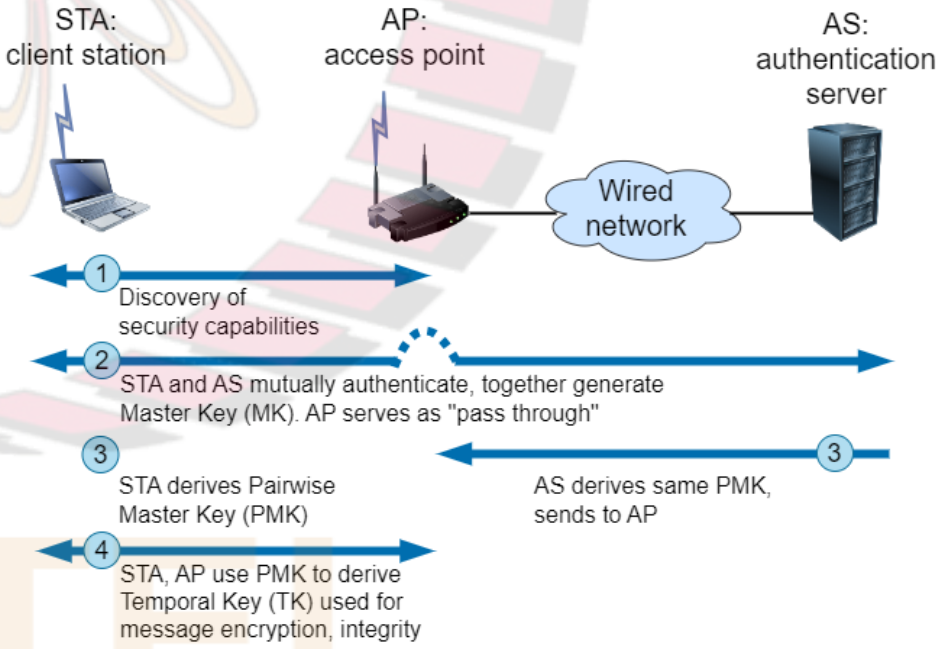


802.11i Operation

- 802.11i operates in four phases:

1) *Discovery*:
   - AP periodically transmits “beacon” packets
   - beacon packet contains list of types of authentication and encryption supported
   - mobile device sends packet to AP, requesting specific forms of authentication and encryption that it wants

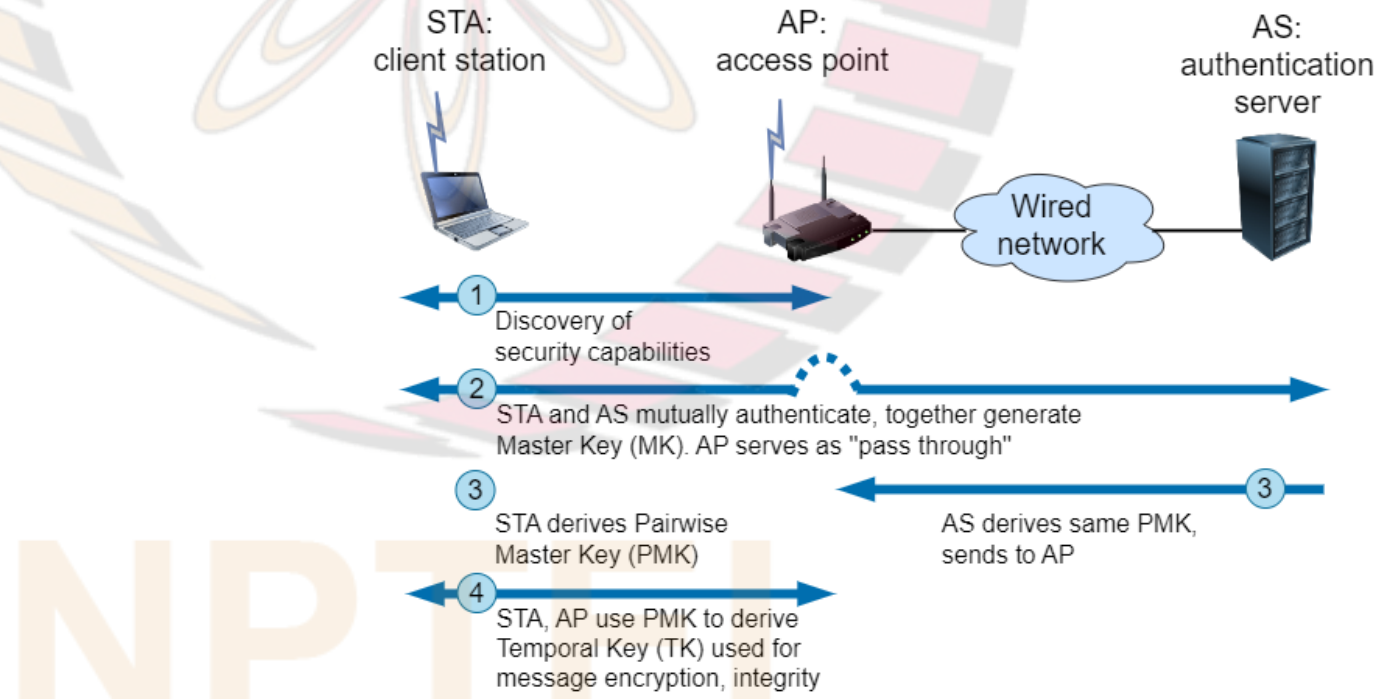
2) and 3) Mutual Authentication:
   - mutual authentication takes place between mobile device and authentication server; AP acts as relay during authentication process
   - protocol used for authentication called “Extensible Authentication Protocol (EAP)”
   - EAP supports multiple authentication protocols; a commonly used protocol is EAP-TLS, which is based on TLS authentication (which we studied earlier and which uses public key techniques and nonces)
   - end result of a successful authentication is a *Pairwise Master Key* (PMK) shared between the mobile device and the authentication server, which the authentication server then conveys to the AP



802.11i Operation

4) *Key Generation*:

- the mobile device and AP use PMK and exchange of two nonces, one in each direction, to derive the *Pairwise Transient Key (PTK)*
- From the PTK, the following are derived:
  - *Temporal Key*, which is used for data encryption and message integrity
  - *Key Confirmation Key (KCK)*
  - *Key Encryption Key (KEK)*



Authentication Methods Supported by EAP

- EAP is not a single authentication protocol, but rather a framework that supports various authentication protocols
- E.g.:
  - EAP-MD5
  - EAP-TLS
  - EAP-TTLS
- EAP-MD5:
  - Authentication server challenges the station to transmit the MD5 hash of the user's password
  - Station prompts user for password and sends its hash to authentication server
  - This protocol is insecure because:
    - Attacker can eavesdrop on above message exchange and later replay the hashed password, thus impersonating the legitimate user
    - Also, authentication is one-way; authentication of server to station is not done

Authentication Methods Supported by EAP (contd.)

- EAP-TLS
  - based on the SSL/ TLS protocol, which we discussed
  - of all the EAP methods, this is the most secure
  - provides mutual authentication and agreement on a master key
  - requires authentication server as well as user (station) to have digital certificates
    - unlike most implementations of TLS used to secure HTTP, *client-side certificates are mandatory*
    - this requirement makes EAP-TLS highly secure; compromised user password not enough to break its security
  - relatively straightforward to equip server with a digital certificate and a corresponding private key
  - however, assigning public-private key pair to each user may not be feasible; this makes it difficult to use EAP-TLS in practice

Authentication Methods Supported by EAP (contd.)

- EAP-TTLS (tunnelled TLS)
  - similar to EAP-TLS; difference is that certificate is only required at the authentication server end
  - server authenticates itself to the station and both sides construct a secure tunnel between themselves
  - over this secure tunnel, station authenticates itself to server by sending its user name and password

802.11i PSK Mode

- The procedure discussed above (using an authentication server) is typically used in large 802.11 networks, such as those deployed in university and corporate campuses
- For 802.11 networks deployed in homes and small offices, a different and simpler procedure is often used:
  - called *Pre-shared Key (PSK)* mode
- If PSK mode is used, shared keys (passwords) are manually installed in APs and informed to users of mobile devices
- The PMK is a function of the PSK; computed independently by mobile device and AP
- When using PSK mode, after computation of the PMK:
  - the mobile device and AP use PMK and exchange of two nonces, one in each direction, to derive the Pairwise Transient Key (PTK); Temporal Key, KEK and KCK are derived from PTK
  - as in authentication server mode