Securing Wireless LANs: Part 8

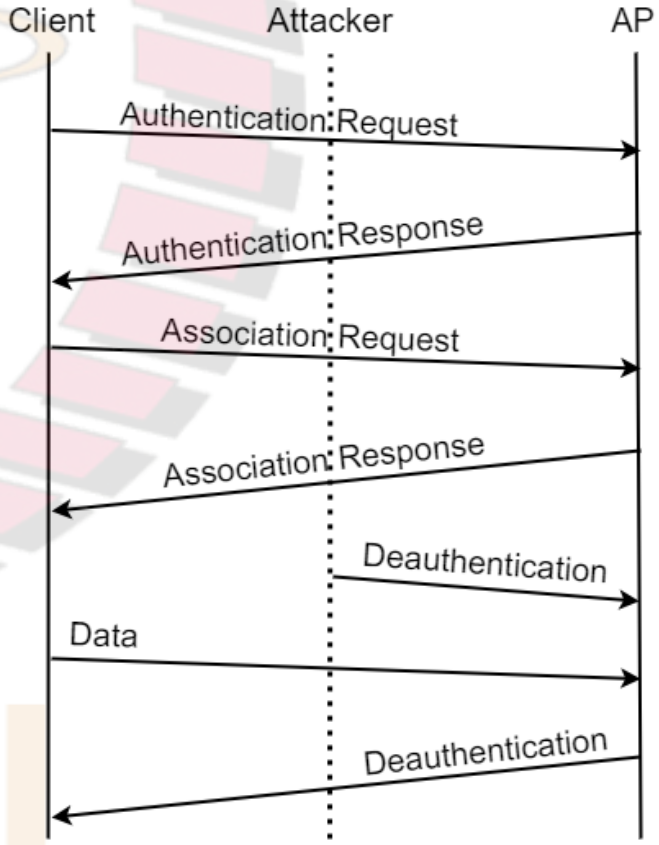
Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- J. Edney, W.A. Arbaugh, "*Real 802.11 Security: Wi-Fi Protected Access and 802.11i*", Pearson Education, 2004.
- J. Bellardo, S. Savage, "802.11 Denial-Of-Service attacks: Real Vulnerabilities and Practical Solutions," In *Proceedings of the 12th conference on USENIX Security Symposium*– Volume12, Pages 15-28, 2003.
- M.S. Ahmad, S. Tadakamadla. "Short paper: security evaluation of IEEE 802.11 w specification", in *Proceedings of the fourth ACM conference on Wireless network security*, pp. 53-58, 2011.
- Wikipedia article on 802.11w:
  - https://en.wikipedia.org/wiki/IEEE_802.11w-2009

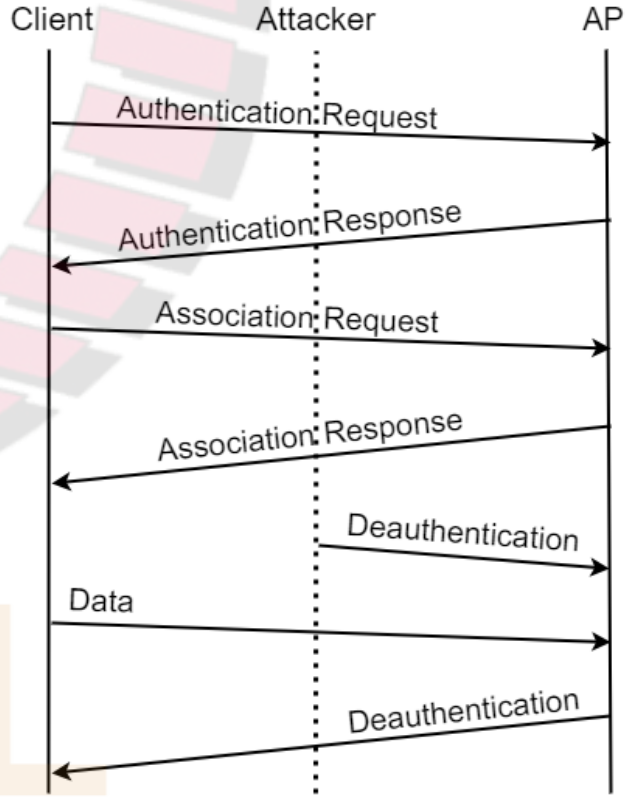
Deauthentication Attack

- Recall: deauthenticate frame allows clients and APs to request deauthentication from one another
- Before 802.11w, no message integrity mechanism was used for this frame
- Consequently the attacker could spoof this frame, either pretending to be the AP or the client, and direct it to the other party (see fig.)
- In response, the recipient (AP or client) would exit the authenticated state and refuse all further packets until authentication was reestablished
- By repeating the attack persistently a client may be kept from transmitting or receiving data indefinitely



Disassociation Attack

- Similar to deauthentication attack
- Recall: before exchanging data packets, client associates with an AP
- 802.11 provides a disassociation message similar to the deauthentication message discussed earlier
- Before 802.11w, no message integrity mechanism was used for disassociation message
- This vulnerability can be exploited by an attacker by sending a disassociation message to client or AP
  - ❑ in response, the recipient (client or AP) would exit the associated state and would refuse all further packets until association was reestablished
- However, note that disassociation attack is less efficient than the deauthentication attack for an attacker
  - ❑ this is because deauthentication forces the victim node to do more work to return to the associated state than does disassociation, ultimately requiring less work on the part of the attacker



Attacks on Power Saving Functions

- To conserve energy, clients are allowed to enter a *sleep state* during which they are unable to transmit or receive
- Before entering the sleep state, the client announces its intention, so the AP can start buffering any inbound traffic for the client
- Occasionally the client awakens and polls the AP for any pending traffic
- If there is any buffered data at this time, the AP delivers it and subsequently discards the contents of its buffer
- Before 802.11w, by spoofing polling message on behalf of client, an attacker could cause the AP to discard the client's packets while it was asleep
- Also, it was potentially possible to trick the client node into thinking there were no buffered packets at the AP when in fact there were:
  - ❑ the presence of buffered packets is indicated in a periodically broadcast packet called the traffic indication map, or TIM
  - ❑ if the TIM message itself is spoofed, an attacker may convince a client that there is no pending data for it and the client will immediately revert back to the sleep state
- Finally, the power conservation mechanisms rely on time synchronization between the AP and its clients so clients know when to awake
  - ❑ key synchronization information, such as the period of TIM packets and a timestamp broadcast by the AP, were sent without message integrity and in the clear
  - ❑ by forging these management packets, an attacker could cause a client node to fall out of sync with the AP and fail to wake up at the appropriate times

IEEE 802.11w

- Recall:
  - ❑ before 802.11w, only data frames could be protected in Wi-Fi and management frames were sent without any protection
  - ❑ due to this, Wi-Fi had several vulnerabilities
- 802.11w amendment provides protection for some management frames
- It uses existing security mechanisms (those standardized in 802.11i) rather than creating new security schemes or new management frame format
  - ❑ these existing security mechanisms are used to protect management frames, in addition to data frames
- It is infeasible to protect the management frames sent before the four-way handshake because they are sent prior to key establishment
- The management frames that are sent after key establishment are protected
- E.g. of management frames that are *not* protected:
  - ❑ Beacon and probe request/ response frames
  - ❑ Authentication request/ response frames
  - ❑ Association request/ response frames
- E.g. of management frames that are protected:
  - ❑ Disassociate frame
  - ❑ Deauthenticate frame

IEEE 802.11w (contd.)

- Protection-capable management frames are protected using the same mechanism as an ordinary data frame:
  - ❑ Payload is encrypted using CCMP
  - ❑ Message integrity is provided for payload and header using CCMP
- As for data frames, the Temporal Key (TK) is used to provide encryption and message integrity
- Replay protection is provided by using the same mechanism as for data frames
- In 2018, WPA3 was announced as a replacement for WPA2
  - ❑ WPA3 makes it mandatory to use management frame protection defined in the 802.11w standard
  - ❑ WPA3 also makes it mandatory to use a protocol called Simultaneous Authentication of Equals (SAE)/ Dragonfly handshake for authentication between the client and AP
    - o details omitted
- Due to management frame protection, attacks discussed above are defended against

Vulnerabilities in 802.11w Networks

- Recall:
  - 802.11w provides protection to several management frames
- However, even in 802.11w networks, some vulnerabilities have been shown to exist
- We now discuss some of them
- Deauthentication attack:
  - 802.11w provides protection to deauthentication frames only after the completion of the four way handshake
  - an attacker can send a spoofed deauthentication packet before this handshake, ending the connection between client and AP
  - if this attack is performed repeatedly, then it results in DoS to the client
- Beacon/ Probe frame flood attack
  - recall: 802.11w does not protect beacons
  - so an attacker can flood the network with a large number of beacons advertising different APs
  - this can confuse clients and make it difficult to find the legitimate AP
  - similarly, recall that 802.11w does not protect probe requests and responses
  - so again, an attacker can flood the network with a large number of probe request or response frames
  - this can waste bandwidth and/ or cause confusion to clients and/ or APs
- Attacks like the above can be defended against using "*Intrusion Detection Systems*"