Global Leader in Wireless Security

Hooray, 802.11w Is Ratified... So, What Does it Mean for Your WLAN?

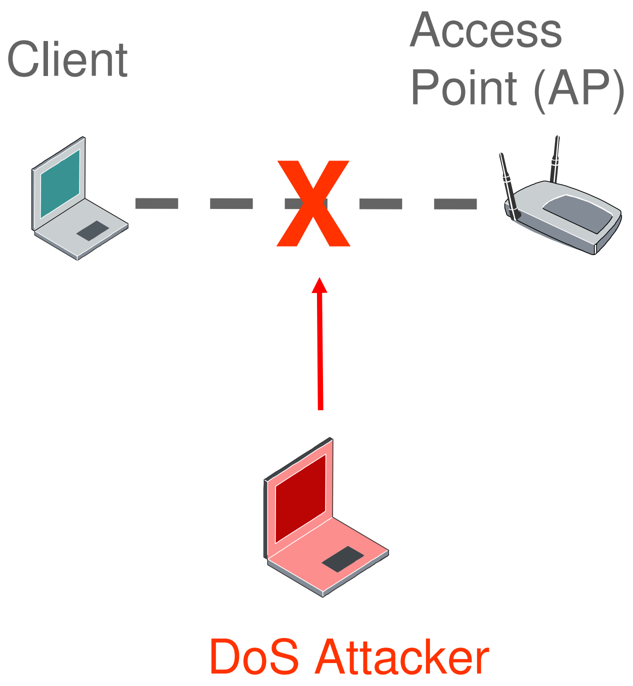
A Brief Tutorial on IEEE 802.11w

Gopinath K N and Hemant Chaskar

AirTight Networks
www.AirTightNetworks.com

Background

- 802.11 WiFi going from "convenience" to "mission critical"
- However, ever since inception, WiFi has been vulnerable to Denial of Service (DoS) attacks of various types:
  - RF Jamming
  - Virtual Jamming
  - Spoofed Disconnect
  - EAP Spoofing
  - Connection Request Flooding
  - etc.



802.11w: A step in the direction of DoS avoidance

- 802.11w gets rid of “Spoofed Disconnect” DoS attacks resulting from spoofing of
  - (i) Deauthentication (Deauth), (ii) Disassociation (Disassoc), (iii) Association (Assoc) Request in existing connection, or (iv) Authentication (Auth) Request in existing connection

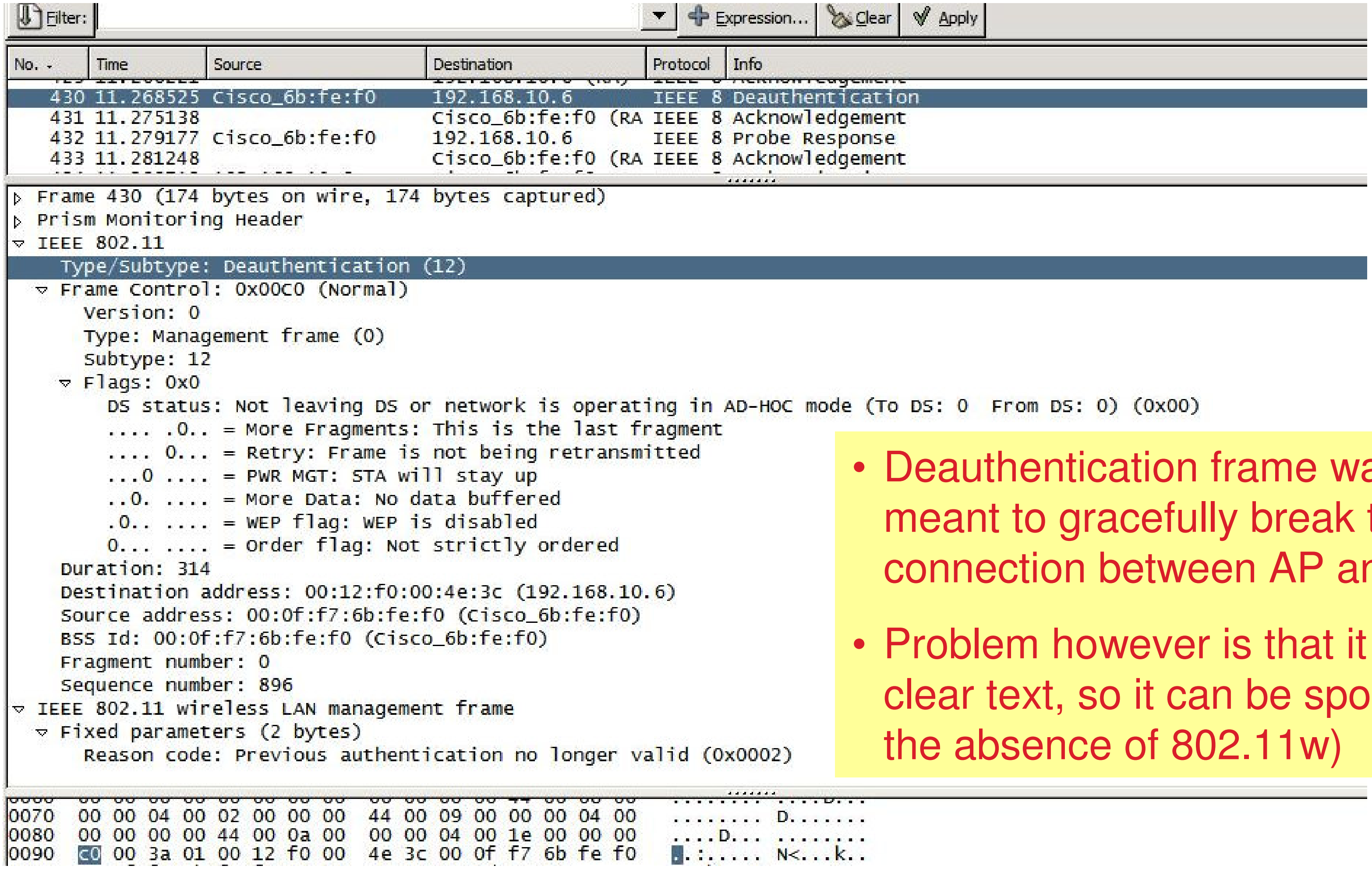
- Certain “Action Management Frames” are also made anti-spoofing
  - Spectrum Management, QoS, BlockAck, Radio Measurement, Fast BSS Transition

How does 802.11w avoid Spoofed Disconnect DoS

- 802.11w adds cryptographic protection to Deauth and Disassoc frames to make them anti-spoofing

- Mechanism called Security Association (SA) teardown protection is added to prevent spoofed Assoc Request or Auth Request from disconnecting the already connected Client

Example: Deauth Attack



```
No.  Time       Source          Destination          Protocol  Info
430 11.268525 Cisco_6b:fe:f0   192.168.10.6          IEEE 8 Deauthentication
431 11.275138                  Cisco_6b:fe:f0 (RA    IEEE 8 Acknowledgement
432 11.279177 Cisco_6b:fe:f0   192.168.10.6          IEEE 8 Probe Response
433 11.281248                  Cisco_6b:fe:f0 (RA    IEEE 8 Acknowledgement
```

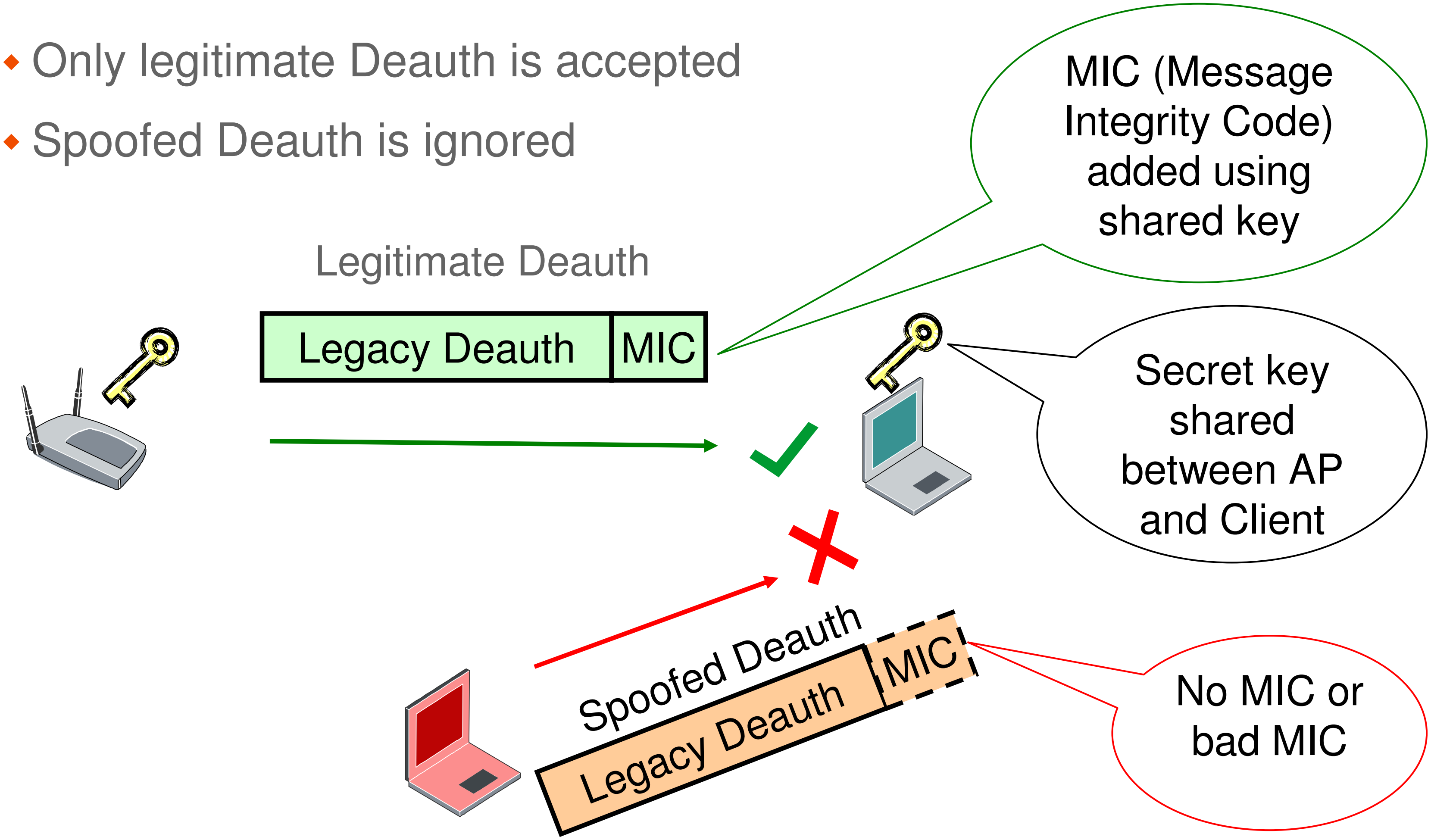
```
▷ Frame 430 (174 bytes on wire, 174 bytes captured)
▷ Prism Monitoring Header
▽ IEEE 802.11
    Type/Subtype: Deauthentication (12)
  ▽ Frame Control: 0x00C0 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 12
    ▽ Flags: 0x0
        DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0  From DS: 0) (0x00)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = WEP flag: WEP is disabled
        0... .... = Order flag: Not strictly ordered
    Duration: 314
    Destination address: 00:12:f0:00:4e:3c (192.168.10.6)
    Source address: 00:0f:f7:6b:fe:f0 (Cisco_6b:fe:f0)
    BSS Id: 00:0f:f7:6b:fe:f0 (Cisco_6b:fe:f0)
    Fragment number: 0
    Sequence number: 896
▽ IEEE 802.11 wireless LAN management frame
  ▽ Fixed parameters (2 bytes)
      Reason code: Previous authentication no longer valid (0x0002)
```

```
0070  00 00 04 00 02 00 00 00  44 00 09 00 00 00 04 00   ........ D.......
0080  00 00 00 00 44 00 0a 00  00 00 04 00 1e 00 00 00   ....D... ........
0090  c0 00 3a 01 00 12 f0 00  4e 3c 00 0f f7 6b fe f0   ..:..... N<...k..
```

- Deauthentication frame was meant to gracefully break the connection between AP and Client
- Problem however is that it is in clear text, so it can be spoofed (in the absence of 802.11w)

Example: Deauth attack averted with 802.11w

- Only legitimate Deauth is accepted
- Spoofed Deauth is ignored



Legitimate Deauth

Legacy Deauth | MIC

MIC (Message Integrity Code) added using shared key

Secret key shared between AP and Client

Spoofed Deauth

Legacy Deauth | MIC

No MIC or bad MIC

Where does the shared secret key come from

- It is derived using EAPOL 4-way handshake between AP and Client
- This also means that 802.11w can only be used if you are using WPA or WPA2
- Broadcast/multicast management frames are protected using a key called Integrity Group Temporal Key (IGTK)
- Unicast management frames are protected using WPA/WPA2 pair-wise encryption key (PTK)

SA teardown protection

- Pre 802.11w, if AP receives Assoc or Auth Request from already associated Client, it terminates existing connection to start a new one
  - So existing connection can be broken with spoofed Auth Request or Assoc Request
- With SA teardown of 802.11w
  - After AP receives Assoc or Auth Request for associated Client,
  - Crypto protected probe is sent to Client
  - If crypto protected response is received, the Assoc or Auth Request is considered spoofed and rejected
  - Else, existing connection is terminated to start a new one

How are Action Mgmt Frames made spoof resistant

- By adding authentication & encryption using IGTK
  - Spectrum Management
  - QoS
  - DLS
  - Block Ack
  - Radio measurement
  - Fast BSS Transition
  - HT
  - SA Query
  - Protected Dual of Public Action

802.11w: A piece in WiFi security puzzle

- 802.11w averts Spoofed Disconnect DoS and makes Action Management Frames spoof-resistant
- Other DoS attacks (RF jamming, virtual jamming, EAP spoofing, connection request flooding etc.) are outside the scope of 802.11w
- WPA/WPA2 is still needed for client authentication and data encryption. Also WPA/WPA2 is needed for 802.11w to work
- Threats from unmanaged devices (rogue APs, mis-associations, ad hoc connections, honeypots (Evil Twin), AP/client MAC spoofing, cracking, infrastructure attacks (skyjacking) etc.) are outside the scope of 802.11w
- You should definitely enable 802.11w in your WLAN when it becomes available (shortly) in WLAN equipment, but one should not be complacent that it will solve all wireless security problems

Questions/comments

Please discuss@

http://blog.airtightnetworks.com/802-11w-tutorial/

Appendix 1: Broadcast Integrity Protocol (BIP)

- Provides authentication and replay protection for broadcast/multicast Management Frames
- Uses “Integrity Group Temporal Key” (IGTK), a new key derived & distributed via EAPOL 4-way handshake
- Transmitter appends each protected frame with a Management MIC Information Element (IE)
- Receiver validates the MIC before accepting the frame

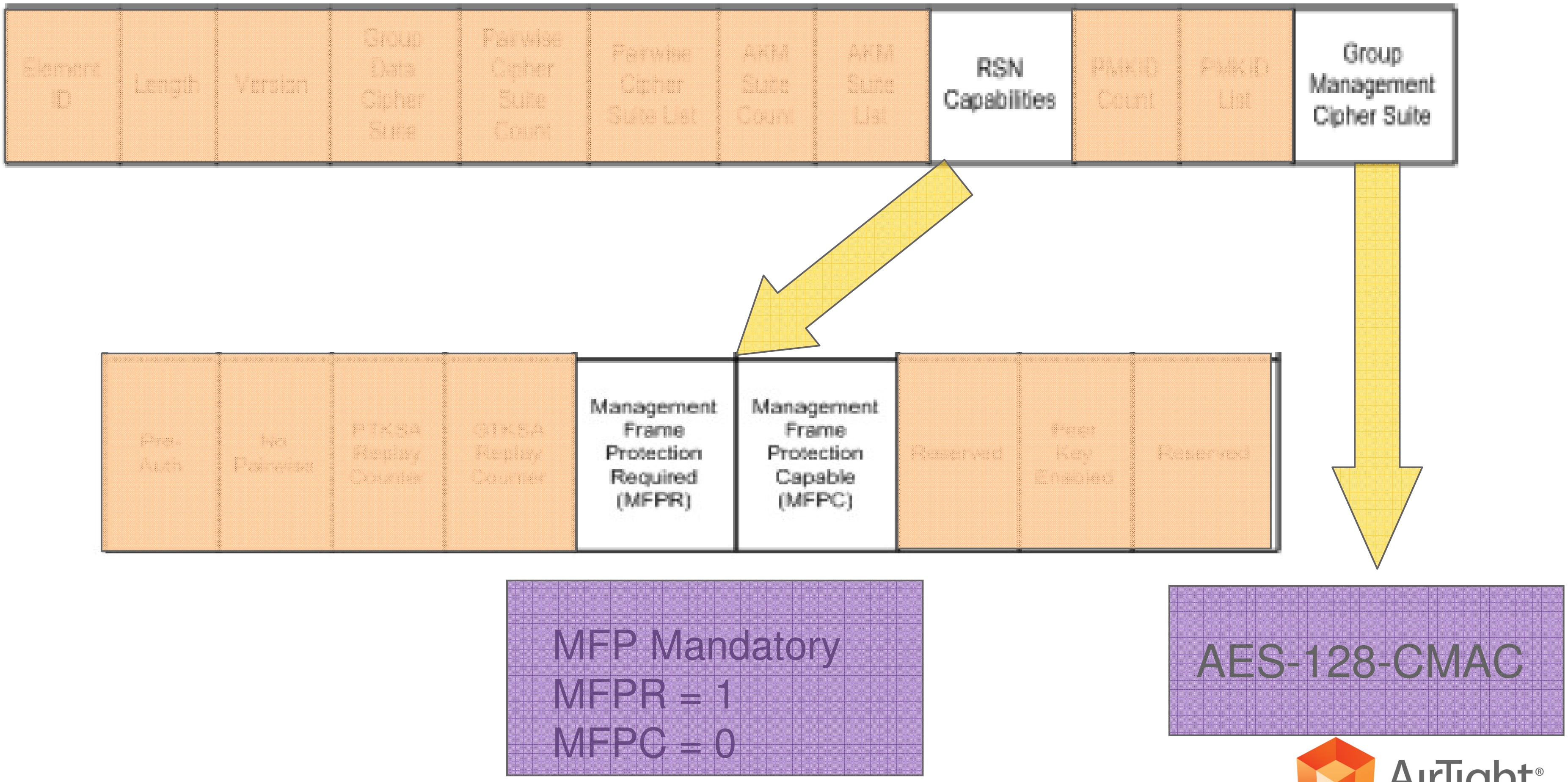
Appendix 2: Message Integrity Check (MIC) IE

ID	Length	Key ID	IPN	MIC

- ID
  - Information Element number
- Key ID
  - Indicates the IGTK used for computing MIC
- IPN
  - Used for replay protection
  - Monotonically increasing non-negative number
- MIC
  - The keyed cryptographic hash derived over management frame body (Payload + MAC header)

Appendix 3: 802.11w parameter negotiation

Negotiated at the beginning of Association



MFP Mandatory
MFPR = 1
MFPC = 0

AES-128-CMAC