

## PCAP Quiz #1 Questionare with answers

### 1. 802.1X/EAP Authentications

Since we have a authentication server (radius-server) in our network the clients will use 802.1X/EAP authentication. Its only one user account configured on the Radius server, so all clients will use the same username and password. All three clients will associate to one of the access points and some of them will roam to another during the capture

#### Question 1.1

Which type of 802.1X/EAP-authentication method is used in this network?

Answer:

Packet number 3 and 4 during 802.1X/EAP authentication in this pcap is where the authentication server and the supplicant negotiate EAP method. First the AS sends it preferred EAP method (Request Protected EAP). Since the supplicant is using PEAP it follow up with the Client Hello

|         |                   |  |
|---------|-------------------|--|
| 5180MHz | Association Re... | Association Request, SN=2050, FN=0, Flags=.....C, SSID=CTK_central_switch. |
| 5180MHz | Association Re... | Association Response, SN=3762, FN=0, Flags=.....C                          |
| 5180MHz | Netw... QoS Data  | Request, Identity  |
| 5180MHz | Voic... QoS Data  | Response, Identity   |
| 5180MHz | Netw... QoS Data  | Request, Protected EAP (EAP-PEAP)  |
| 5180MHz | Voic... QoS Data  | Client Hello   |
| 5180MHz | Netw... QoS Data  | Server Hello, Certificate, Server Key Exchange, Server Hello Done          |
| 5180MHz | Voic... QoS Data  | Response, Protected EAP (EAP-PEAP)   |
| 5180MHz | Netw... QoS Data  | Server Hello, Certificate, Server Key Exchange, Server Hello Done          |
| 5180MHz | Voic... QoS Data  | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message       |
| 5180MHz | Netw... QoS Data  | Change Cipher Spec, Encrypted Handshake Message                            |

|  |
|--|
| <  |
| > Frame 4346: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0 |
| > Radiotap Header v0, Length 32  |
| > 802.11 radio information   |
| > IEEE 802.11 QoS Data, Flags: .....F.C  |
| > Logical-Link Control   |
| > 802.1X Authentication  |
| ▼ Extensible Authentication Protocol   |
| Code: Request (1)  |
| Id: 2  |
| Length: 6  |
| Type: Protected EAP (EAP-PEAP) (25)  |
| ▼ EAP-TLS Flags: 0x20  |
| 0... .... = Length Included: False   |
| .0.. .... = More Fragments: False  |
| ..1. .... = Start: True  |
| .... .000 = Version: 0   |

## Question 1.2

In several 802.1X/EAP authentication methods the supplicant sends a “bogus” outer identity. What is the “bogus” outer identity for these clients? Could that outer identity also be its real username?

Answer

Packet number 1 and 2 in the 802.1X/EAP authentication are Request Identity from the AS and Response Identity from the supplicant. The Response Identity brings a “bogus” Identity (gjermund).

Yes it could also be the real username, but the actual username/password exchange is done during the inner EAP method. In this pcap this is happening during the eight Application Data packets

|         |                   |  |
|---------|-------------------|--|
| 5180MHz | Association Re... | Association Response, SN=3762, FN=0, Flags=.....C                    |
| 5180MHz | Netw... QoS Data  | Request, Identity  |
| 5180MHz | Voic... QoS Data  | Response, Identity   |
| 5180MHz | Netw... QoS Data  | Request, Protected EAP (EAP-PEAP)                                    |
| 5180MHz | Voic... QoS Data  | Client Hello   |
| 5180MHz | Netw... QoS Data  | Server Hello, Certificate, Server Key Exchange, Server Hello Done    |
| 5180MHz | Voic... QoS Data  | Response, Protected EAP (EAP-PEAP)                                   |
| 5180MHz | Netw... QoS Data  | Server Hello, Certificate, Server Key Exchange, Server Hello Done    |
| 5180MHz | Voic... QoS Data  | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 5180MHz | Netw... QoS Data  | Change Cipher Spec, Encrypted Handshake Message                      |

<

> Frame 4345: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0

> Radiotap Header v0, Length 32

> 802.11 radio information

> IEEE 802.11 QoS Data, Flags: .....TC

> Logical-Link Control

> 802.1X Authentication

▼ Extensible Authentication Protocol

Code: Response (2)

Id: 1

Length: 13

Type: Identity (1)

Identity: gjermund

### Question 1.3

During the 802.1X/EAP authentication the supplicant sends its Cipher Suite capabilities. How many Cipher Suites are the Samsung A5 capable of?

Answer:

During 802.1X/EAP authentication the supplicant sends its cipher suites capabilities in the Client Hello packet. In the SSL section of the packet are the Cipher suites transferred. The Samsung A5 are capable to do 30 different cipher suites

|         |         |          |  |
|---------|---------|----------|--|
| 5180MHz | Netw... | QoS Data | Association Response, SN=3702, FN=0, Flags=.....TC                   |
| 5180MHz | Netw... | QoS Data | Request, Identity  |
| 5180MHz | Voic... | QoS Data | Response, Identity   |
| 5180MHz | Netw... | QoS Data | Request, Protected EAP (EAP-PEAP)                                    |
| 5180MHz | Voic... | QoS Data | Client Hello   |
| 5180MHz | Netw... | QoS Data | Server Hello, Certificate, Server Key Exchange, Server Hello Done    |
| 5180MHz | Voic... | QoS Data | Response, Protected EAP (EAP-PEAP)                                   |
| 5180MHz | Netw... | QoS Data | Server Hello, Certificate, Server Key Exchange, Server Hello Done    |
| 5180MHz | Voic... | QoS Data | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 5180MHz | Netw... | QoS Data | Change Cipher Spec, Encrypted Handshake Message                      |
| 5180MHz | Voic... | QoS Data | Response, Protected EAP (EAP-PEAP)                                   |
| 5180MHz | Netw... | QoS Data | Application Data   |
| 5180MHz | Voic... | QoS Data | Application Data   |

|  |
|--|
| Version: TLS 1.0 (0x0301)  |
| Length: 152  |
| Handshake Protocol: Client Hello                                     |
| Handshake Type: Client Hello (1)                                     |
| Length: 148  |
| Version: TLS 1.2 (0x0303)  |
| Random: 29da6f741cc8eb6238d957c30a7ced6e28986ea7caaabfb1...          |
| Session ID Length: 0   |
| Cipher Suites Length: 60   |
| Cipher Suites (30 suites)  |
| Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)       |
| Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)         |
| Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)           |
| Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)       |
| Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)         |
| Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)           |
| Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) |
| Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)   |

#### Question 1.4

In response to the supplicant Cipher Suite capabilities, the Authentication server decide to use one of the Cipher suite. Which one is used between the Samsung A5 and AP?

Answer:

The packet straight after the supplicant has announced its cipher suites (Client Hello), the AS tells which to use in the frame Server Hello (Server Hello, Certificate, Server Key Exchange, Server Hello Done)

The authentications server has decided to use

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

What that means is out of the scope, but look at Brian Longs presentation at WLPC\_US 2019

|         |                   |  |
|---------|-------------------|--|
| 5180MHz | Association Re... | Association Response, SN=3762, FN=0, Flags=.....C                    |
| 5180MHz | Netw... QoS Data  | Request, Identity  |
| 5180MHz | Voic... QoS Data  | Response, Identity   |
| 5180MHz | Netw... QoS Data  | Request, Protected EAP (EAP-PEAP)                                    |
| 5180MHz | Voic... QoS Data  | Client Hello   |
| 5180MHz | Netw... QoS Data  | Server Hello, Certificate, Server Key Exchange, Server Hello Done    |
| 5180MHz | Voic... QoS Data  | Response, Protected EAP (EAP-PEAP)                                   |
| 5180MHz | Netw... QoS Data  | Server Hello, Certificate, Server Key Exchange, Server Hello Done    |
| 5180MHz | Voic... QoS Data  | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 5180MHz | Netw... QoS Data  | Change Cipher Spec, Encrypted Handshake Message                      |
| 5180MHz | Voic... QoS Data  | Response, Protected EAP (EAP-PEAP)                                   |
| 5180MHz | Netw... QoS Data  | Application Data   |
| 5180MHz | Voic... QoS Data  | Application Data   |

[Fragment Count: 2]

[Reassembled EAP-TLS Length: 1118]

Secure Sockets Layer

- TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 57
  - Handshake Protocol: Server Hello
    - Handshake Type: Server Hello (2)
    - Length: 53
    - Version: TLS 1.2 (0x0303)
    - Random: 782d9691121cdff94ec7f95057e0e6c45dd09d5cc334e680...
    - Session ID Length: 0
    - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)
    - Compression Method: null (0)
    - Extensions Length: 13

### Question 1.5

Does the Samsung A5 and the iPad use the same cipher suite?

Answer:

No, the connection to the iPad uses TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 while the connection to the Samsung A5 uses TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Why the difference,; out of scope

|         |                   |  |
|---------|-------------------|--|
| 5180MHz | Association Re... | Association Request, SN=3620, FN=0, Flags=.....C, SSID=CTK_central_switching |
| 5180MHz | Association Re... | Association Response, SN=950, FN=0, Flags=.....C                             |
| 5180MHz | Voic... QoS Data  | Request, Identity  |
| 5180MHz | Best... QoS Data  | Response, Identity   |
| 5180MHz | Voic... QoS Data  | Request, Protected EAP (EAP-PEAP)  |
| 5180MHz | Best... QoS Data  | Client Hello   |
| 5180MHz | Voic... QoS Data  | Server Hello, Certificate, Server Key Exchange, Server Hello Done            |
| 5180MHz | Best... QoS Data  | Response, Protected EAP (EAP-PEAP)   |
| 5180MHz | Voic... QoS Data  | Server Hello, Certificate, Server Key Exchange, Server Hello Done            |
| 5180MHz | Best... QoS Data  | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message         |
| 5180MHz | Voic... QoS Data  | Change Cipher Spec, Encrypted Handshake Message                              |

[Fragment Count: 2]

[Reassembled EAP-TLS Length: 1118]

Secure Sockets Layer

- TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 57
  - Handshake Protocol: Server Hello
    - Handshake Type: Server Hello (2)
    - Length: 53
    - Version: TLS 1.2 (0x0303)
    - Random: f41ee19d027c2e8e5dc643ddcec967061d53913f22e9cd46...
    - Session ID Length: 0
    - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)
    - Compression Method: null (0)
    - Extensions Length: 13

## 2. Fast roaming

The network is configured with both 803.11i (WPA) and 803.11r (BSS FT) roaming methods

### Question 2.1

There are three different supplicants that connects to the network. Which ones supports 803.11r (BSS FT) and which ones supports only 802.11i (WPA)

Answer:

First of all. If we look at the beacon for this SSID and its RSN IE we will see that this SSID support two different authentications key management suites (AKM), both FT over IEEE 802.1X and WPA  
And the beacon also contains the Mobility Domain IE

```
36 44 5180MHz Beacon frame Beacon frame, SN=3129, FN=0, Flags=.....C, BI=100, SSID=CTK_central_switching
36 5180MHz Beacon frame Beacon frame, SN=818, FN=0, Flags=.....C, BI=102, SSID=CTK_central_switching
36 36 5180MHz Beacon frame Beacon frame, SN=3341, FN=0, Flags=.....C, BI=100, SSID=CTK_central_switching
36 5180MHz Beacon frame Beacon frame, SN=3358, FN=0, Flags=.....C, BI=100, SSID=CTK_central_switching

Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 24
  RSN Version: 1
  > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 2
  > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
  > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
  > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
  > RSN Capabilities: 0x0028
  > Tag: Mobility Domain
    Tag Number: Mobility Domain (54)
    Tag length: 3
    Mobility Domain Identifier: 0x2d45
    FT Capability and Policy: 0x00
    ....0 = Fast BSS Transition over DS: 0x0
    ....0 = Resource Request Protocol Capability: 0x0
  > Tag: HT Information (802.11n D1.10)
    Tag Number: HT Information (802.11n D1.10) (61)
```

Next we go to each clients Association Request frame and the RSN IE. The iPad and the Samsung A5 has AKM suite FT over IEEE 802.1X and the Mobility Domain IE, while the MacBook Pro reports AKM suite WPA.

So the iPad and the Samsung supports 803.11r or BSS Fast transition, while the MacBook Pro only support roaming with WPA using Opportunistic Key Caching (OKC)

## Question 2.2

During the Samsung A5s first association to one of the access point there are some missing packets in the packet capture. Is that a problem? Do you think the A5 did connect? Why are there some missing packets?

answer

Remember that the setup was on a 80MHz channel and with 4 different 20MHz Aps. The three clients was also pinging the default gateway during the capture. So it is very likely that a transmission on another channel is captured by the NIC and our packet is therefor not captured.

In a real scenario this is very likely and it is very depended of the capturing NICs position regarding the other stations in the network

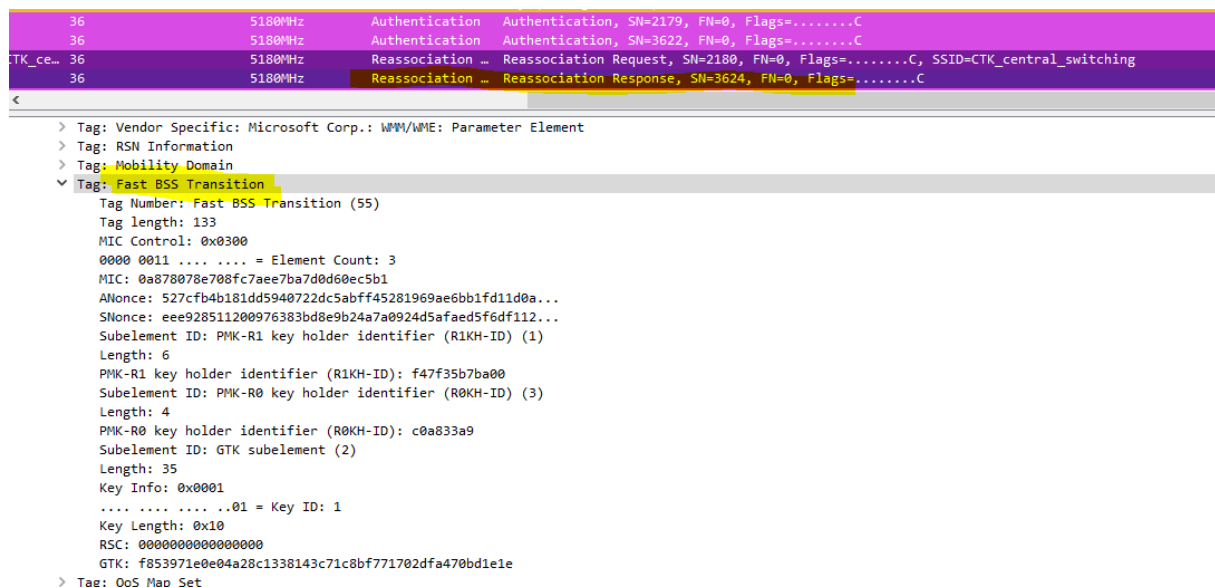
Since it is none packets pointing to something went wrong we could suppose that the client and the AP connected together. If we had looked into the full capture of 100 000 frames we would have seen that the client worked well. Otherwise the client would have associate once more

## Question 2.3

During the packet capture the Samsung A5 first did a full 802.1X/EAP authentication to the first AP, then it roam to another AP without any EAPOL-packets (packet 3730-3737). What happens here?

Answer:

This is roaming with 803.11r. The supplicant and the authenticator (AP) uses the information in the Mobility Domain IE to find out that they have the right keys available and uses the Fast BSS Transition IE to transfer the same data that the 4-way handshake did during initial associations. So instead of either full 802.1X/EAP authentication and the 4-way handshake or only 4-way handshake, the encrypting keys is generated during the four authentications and reassociations frames. This frames is called FT-authentication and FT-reassociation frames, but Wireshark does not tell it



#### Question 2.4

14 seconds after the previous roam, the Samsung A5 associate the same access point. This time with full 802.1X/EAP authentication (start at packet 4340). Why did it happens?

Answer:

The Samsung A5 did a fast roam with 803.11r during packet 3730-3737 to the AP with mac address ending with 1f and associate to the same AP with full 802.1X/EAP authentication starting with packet 4340

If we look at packet 3975 we see that the client sends a Deauthentication to the AP with reason code

“Reason code: Deauthenticated because sending STA is leaving (or has left) IBSS or ESS (0x0003)”

Why: For some other reason the client was not happy and want to try to join again???

|         |                   |  |
|---------|-------------------|--|
| 5180MHz | Action            | Action, SN=3626, FN=0, Flags=.....C  |
| 5180MHz | Action            | Action, SN=765, FN=0, Flags=.....C   |
| 5180MHz | Deauthentication  | Deauthentication, SN=2181, FN=0, Flags=.....C                                      |
| 5180MHz | Probe Request     | Probe Request, SN=2048, FN=0, Flags=.....C, SSID=CTK_central_switching             |
| 5180MHz | Probe Response    | Probe Response, SN=3006, FN=0, Flags=....R...C, BI=102, SSID=CTK_central_switching |
| 5180MHz | Probe Response    | Probe Response, SN=3006, FN=0, Flags=....R...C, BI=102, SSID=CTK_central_switching |
| 5180MHz | Authentication    | Authentication, SN=2049, FN=0, Flags=.....C  |
| 5180MHz | Authentication    | Authentication, SN=3761, FN=0, Flags=.....C  |
| 5180MHz | Association Re... | Association Request, SN=2050, FN=0, Flags=.....C, SSID=CTK_central_switching       |
| 5180MHz | Association Re... | Association Response, SN=3762, FN=0, Flags=.....C                                  |
| 5180MHz | Netw...           | QoS Data Request, Identity   |

<

> Frame 3975: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0

> Radiotap Header v0, Length 32

> 802.11 radio information

> IEEE 802.11 Deauthentication, Flags: .....C

> IEEE 802.11 wireless LAN

> Fixed parameters (2 bytes)

Reason code: Deauthenticated because sending STA is leaving (or has left) IBSS or ESS (0x0003)

#### Question 2.5

Does this network support fast transition over the air or over the DS?

Answer:

The Mobility Domain IE in all the beacons and in probe response and associations response frames to supplicants that support 803.11r has a field FT Capability and Policy. Here is the Fast BSS Transition over DS bit set to “0”, which means FT over the Air

| wlan.fc.type_subtype==1 |           |          |                   |   |
|-------------------------|-----------|----------|-------------------|---|
| Current Channel         | Frequency | Priority | Type/Subtype      | Info  |
| 5180MHz                 |           |          | Association Re... | Association Response, SN=1624, FN=0, Flags=.....C |
| 5180MHz                 |           |          | Association Re... | Association Response, SN=3762, FN=0, Flags=.....C |
| 5180MHz                 |           |          | Association Re... | Association Response, SN=950, FN=0, Flags=.....C  |

<

> Ac Parameters ACI 1 (Background), ACM no, AIFSN 7, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0

> Ac Parameters ACI 2 (Video), ACM no, AIFSN 2, ECWmin/max 3/4 (CWmin/max 7/15), TXOP 94

> Ac Parameters ACI 3 (Voice), ACM no, AIFSN 2, ECWmin/max 2/3 (CWmin/max 3/7), TXOP 47

> Tag: Mobility Domain

Tag Number: Mobility Domain (54)

Tag length: 3

Mobility Domain Identifier: 0x2d45

FT Capability and Policy: 0x00

.... ..0 = Fast BSS Transition over DS: 0x0

.... ..0 = Resource Request Protocol Capability: 0x0

> Tag: Fast BSS Transition