
Laboratoire #1

SWI 2023

Alexandre Jaquier, Géraud Silvestri, Francesco Monti

25.03.2023



Contents

Partie 1 : Beacons, authentication	2
1. Deauthentication attack	2
Question a)	2
Question b)	3
2. Fake channel evil tween attack	3
Question a)	3
3. SSID flood attack	4
Partie 2 : Probes	5
4. Probe Request Evil Twin Attack	5
5. Détection de clients et réseaux	5
Question a)	5
Question b)	6
6. Hidden SSID reveal	6

Partie 1 : Beacons, authentication

1. Deauthentication attack

Question a)

Quel code est utilisé par aircrack pour déauthentifier un client 802.11. Quelle est son interprétation ?

```

CH 5 ][ Elapsed: 48 s ][ 2023-03-28 12:13 ][ enabled AP selection
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
C4:04:15:16:A2:8C -62 0 389 2129 46 5 270 WPA2 COMP PSK FBI-tracking-van_EXT
2C:79:D7:6C:31:0C -71 93 286 869 26 5 485 WPA2 COMP PSK FBI-tracking-van

BSSID STATION PWR Rate Lost Frames Notes Probes
(not associated) BE:FC:E3:05:10:38 -66 0 - 1 0 1
(not associated) 72:74:76:3F:EC:6D -72 0 - 1 0 1 RamoLoss
(not associated) 8A:C1:1A:15:89:45 -8 0 - 1 0 2
(not associated) 8E:87:8F:22:85:F0 -8 0 - 1 0 2 csls9
(not associated) 86:E8:45:1E:9C:80 -4 0 - 1 0 1
(not associated) E0:06:E0:31:AC:D4 -72 0 - 1 0 11 unconfigured
(not associated) D4:1B:81:4F:BB:61 -80 0 - 1 0 1 wrc-38746
C4:04:15:16:A2:8C AE:6C:23:3A:37:9A -74 0 - 1 0 1588 FBI-tracking-van_EXT
C4:04:15:16:A2:8C 1C:91:88:D7:4B:86 -62 1e- 1 5 2324
2C:79:D7:6C:31:0C C4:04:15:16:A2:8C -62 11e- 1e 0 18
2C:79:D7:6C:31:0C 02:0F:85:D7:4B:86 -62 11e- 11e 35 819
2C:79:D7:6C:31:0C 02:0F:85:3A:37:9A -52 1e- 1e 0 30

12:13:32 Waiting for beacon frame (BSSID: C4:04:15:16:A2:8C) on channel 5
12:13:33 Sending 64 directed DeAuth (code 7). STMAC: [AE:6C:23:3A:37:9A] [64]55 ACKs]
12:13:33 Sending 64 directed DeAuth (code 7). STMAC: [AE:6C:23:3A:37:9A] [21]47 ACKs]
12:13:34 Sending 64 directed DeAuth (code 7). STMAC: [AE:6C:23:3A:37:9A] [66]51 ACKs]
12:13:34 Sending 64 directed DeAuth (code 7). STMAC: [AE:6C:23:3A:37:9A] [55]50 ACKs]
12:13:35 Sending 64 directed DeAuth (code 7). STMAC: [AE:6C:23:3A:37:9A] [59]54 ACKs]
12:13:35 Sending 64 directed DeAuth (code 7). STMAC: [AE:6C:23:3A:37:9A] [61]51 ACKs]
12:13:36 Sending 64 directed DeAuth (code 7). STMAC: [AE:6C:23:3A:37:9A] [ 7]67 ACKs]
12:13:36 Sending 64 directed DeAuth (code 7). STMAC: [AE:6C:23:3A:37:9A] [ 3]62 ACKs]
12:13:37 Sending 64 directed DeAuth (code 7). STMAC: [AE:6C:23:3A:37:9A] [13]60 ACKs]
12:13:38 Sending 64 directed DeAuth (code 7). STMAC: [AE:6C:23:3A:37:9A] [ 5]63 ACKs]
  
```

Figure 1: Commande pour déauthentifier un client

On utilise `aireplay-ng` pour déauthentifier un client 802.11. Le code utilisé est 7, qui correspond à Deauthentication because sending STA is leaving (or has left) IBSS or ESS (cf. IEEE 802.11-2016).

A l'aide d'un filtre d'affichage, essayer de trouver d'autres trames de déauthentification dans votre capture. Avez-vous en trouvé d'autres ? Si oui, quel code contient-elle et quelle est son interprétation ?

Les trames de déauthentification que nous avons trouvées sont les suivantes :

```

15192 359.827817381 6a:bb:0c:ef:ef:af 12:fe:1f:dd:54:94 802.11 44 Deauthentication, SN=1138, FN=0, Flags=.....
15200 359.834215291 6a:bb:0c:ef:ef:af 12:fe:1f:dd:54:94 802.11 44 Deauthentication, SN=1139, FN=0, Flags=.....
15324 362.876955320 6a:bb:0c:ef:ef:af 12:fe:1f:dd:54:94 802.11 44 Deauthentication, SN=1140, FN=0, Flags=.....
15327 362.877224475 6a:bb:0c:ef:ef:af 12:fe:1f:dd:54:94 802.11 44 Deauthentication, SN=1140, FN=0, Flags=.....

> Frame 15200: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface wlan1mon, id 0
> Radiotap Header v0, Length 18
> 802.11 radio information
> IEEE 802.11 Deauthentication, Flags: .....
> IEEE 802.11 Wireless Management
  > Fixed parameters (2 bytes)
    Reason code: Class 2 frame received from nonauthenticated STA (0x0006)
  
```

Figure 2: Capture Wireshark

Le code 6 signifie que la STA a reçu une trame de déauthentification de la part de l'AP. La STA a donc été déconnectée de l'AP.

Question b)

Quels codes/raisons justifient l'envoi de la trame à la STA cible et pourquoi ?

- Code 1: Unspecified reason -> La STA a reçu une trame de déauthentification sans raison spécifique.
- Code 4: Disassociated because sending STA is leaving (or has left) BSS -> La STA a reçu une trame de déauthentification car elle a quitté le réseau.
- Code 5: Disassociated because AP is unable to handle all currently associated STAs -> La STA a reçu une trame de déauthentification car l'AP n'est pas capable de gérer toutes les STA associées.

Quels codes/raisons justifient l'envoi de la trame à l'AP et pourquoi ?

- Code 1: Unspecified reason -> L'AP a reçu une trame de déauthentification sans raison spécifique.
- Code 8: Disassociated because sending STA is leaving (or has left) BSS -> L'AP a reçu une trame de déauthentification car la STA a quitté le réseau.

Comment essayer de déauthentifier toutes les STA ?

On peut utiliser l'adresse MAC FF:FF:FF:FF:FF:FF comme adresse MAC de destination car elle va être retransmise à toutes les STA (broadcast). Donc toutes les stations connectées à l'AP vont recevoir la trame de déauthentification.

Quelle est la différence entre le code 3 et le code 8 de la liste ?

Le code 3 signifie que la STA a reçu une trame de déauthentification de la part de l'AP. La STA a donc été déconnectée de l'AP. Le code 8 signifie que l'AP a reçu une trame de déauthentification de la part de la STA. L'AP a donc déconnecté la STA.

Expliquer l'effet de cette attaque sur la cible

L'attaque va déconnecter la cible de l'AP. La cible ne pourra plus se connecter à l'AP tant que l'attaque n'est pas arrêtée et que la cible ne s'est pas reconnectée.

Script : deauth.py

2. Fake channel evil tween attack**Question a)**

Expliquer l'effet de cette attaque sur la cible

L'attaque va simuler un réseau WiFi avec le même SSID que le réseau cible. La cible va donc se connecter au réseau WiFi faux et va donner ses identifiants au faux AP. Le faux AP va ensuite intercepter les données de la cible et les envoyer au vrai AP. Le vrai AP va donc recevoir les données de la cible sans que la cible ne s'en rende compte.

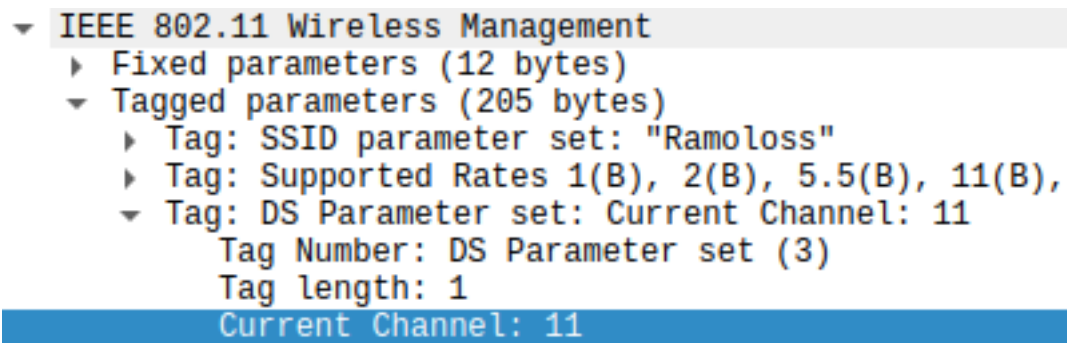


Figure 3: Capture Wireshark de l'AP avant l'attaque

```
Δ > ~ / Doc / H / S / HEIGVD-SWI23-Labo1-MAC-Sec / scripts > main *1 l1 ?1 sudo python 2_fakechannel.py
Nom de l'interface : wlan1mon
Interface sélectionnée : wlan1mon
No BSSID SSID Channel Strength
1 2c:54:2d:38:c1:18 Ramoloss 11 -77
2 1c:24:cd:00:71:70 qwl-51821 11 -83
3 2c:54:2d:38:c6:b4 Ramoloss 11 -75
4 a8:d3:f7:72:65:9f hue-88619 11 -79
5 e6:57:40:cf:85:11 UPC Wi-Free 11 -81
6 36:2c:a4:85:ce:7a UPC Wi-Free 11 -81
7 a0:b5:49:04:04:2c Swisscom 11 -77
8 34:2c:c4:85:ce:7a UPC2170263 11 -81
9 e4:57:40:cf:85:51 UPC5222602 11 -79
Numero du SSID à modifier : 1
No choisi : 1
Channel : 4
.....
Sent 135 packets.
```

Figure 4: Script de l'attaque

Script : fakechannel.py

3. SSID flood attack

TODO: Ajouter le script

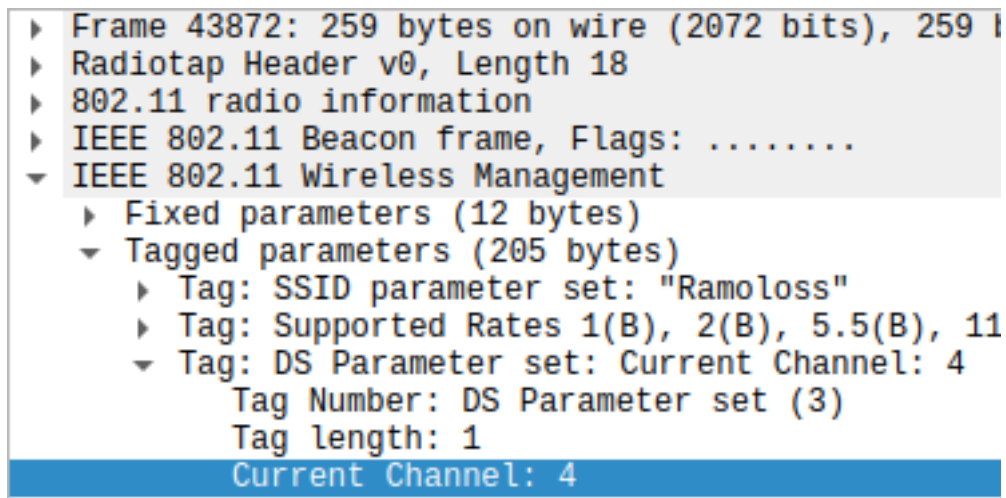


Figure 5: Capture Wireshark de l'AP après l'attaque

Partie 2 : Probes

4. Probe Request Evil Twin Attack

Comment ça se fait que ces trames puissent être lues par tout le monde ? Ne serait-il pas plus judicieux de les chiffrer ?

Les trames *Probe Request* doivent être en clair pour que les AP puissent les lire et savoir si un client est à proximité. Si les trames étaient chiffrées, les AP ne pourraient pas forcément les lire et donc ne pourraient pas envoyer de trames *Probe Response* en retour.

Pourquoi les dispositifs iOS et Android récents ne peuvent-ils plus être tracés avec cette méthode ?

Les dispositifs iOS et Android utilisent des adresses MAC aléatoires pour les trames *Probe Request*. Ceci rend le traçage des dispositifs iOS et Android plus difficile.

TODO: Ajouter le script

5. Détection de clients et réseaux

Question a)

TODO: Ajouter le script

Question b)

TODO: Ajouter le script

6. Hidden SSID reveal

Expliquer en quelques mots la solution que vous avez trouvée pour ce problème ?

TODO: Ajouter le script