

Wifi Protocol 3

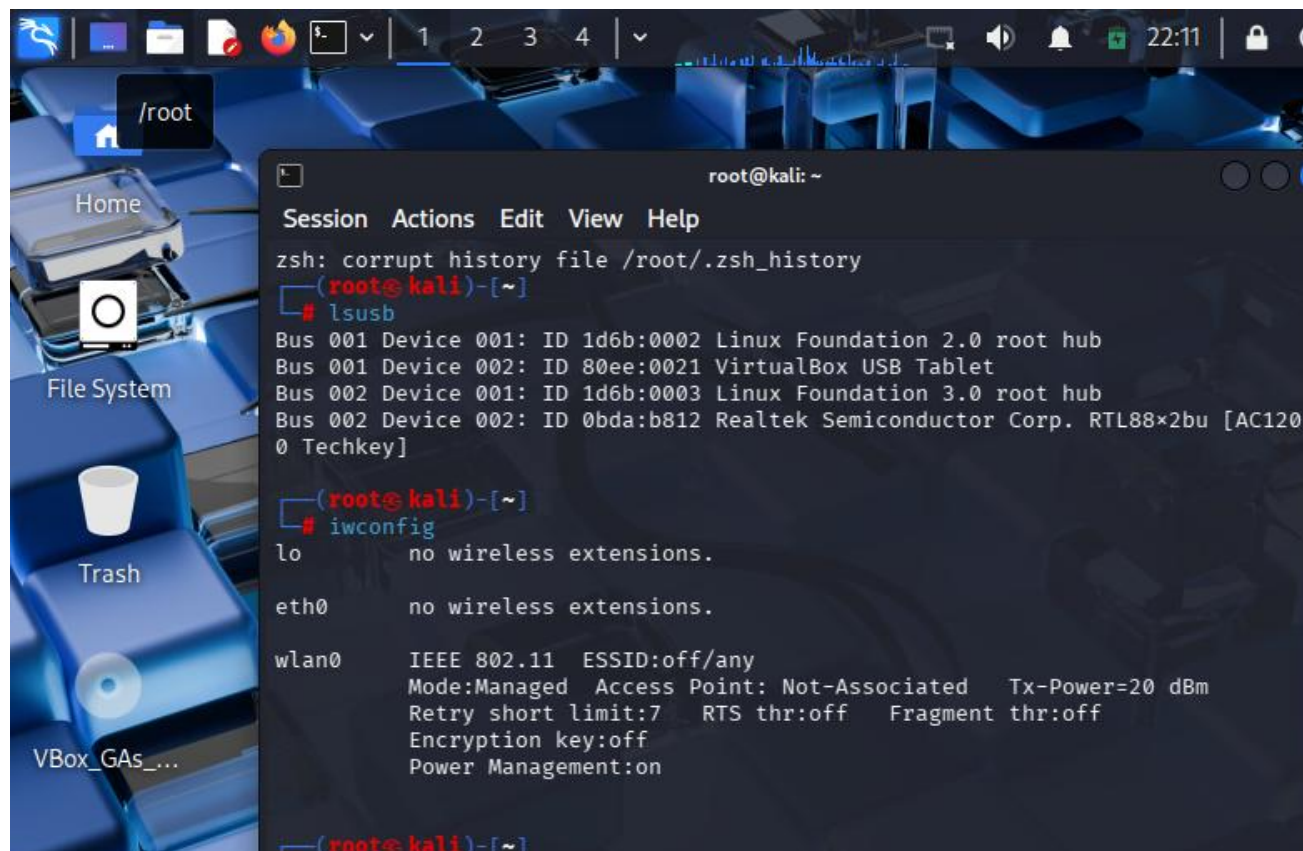
20210638 최무송

TODO

- Fragattacks
- KRACK (Key Reinstallaion AttaCK)
- PMKID offline dictionary attack

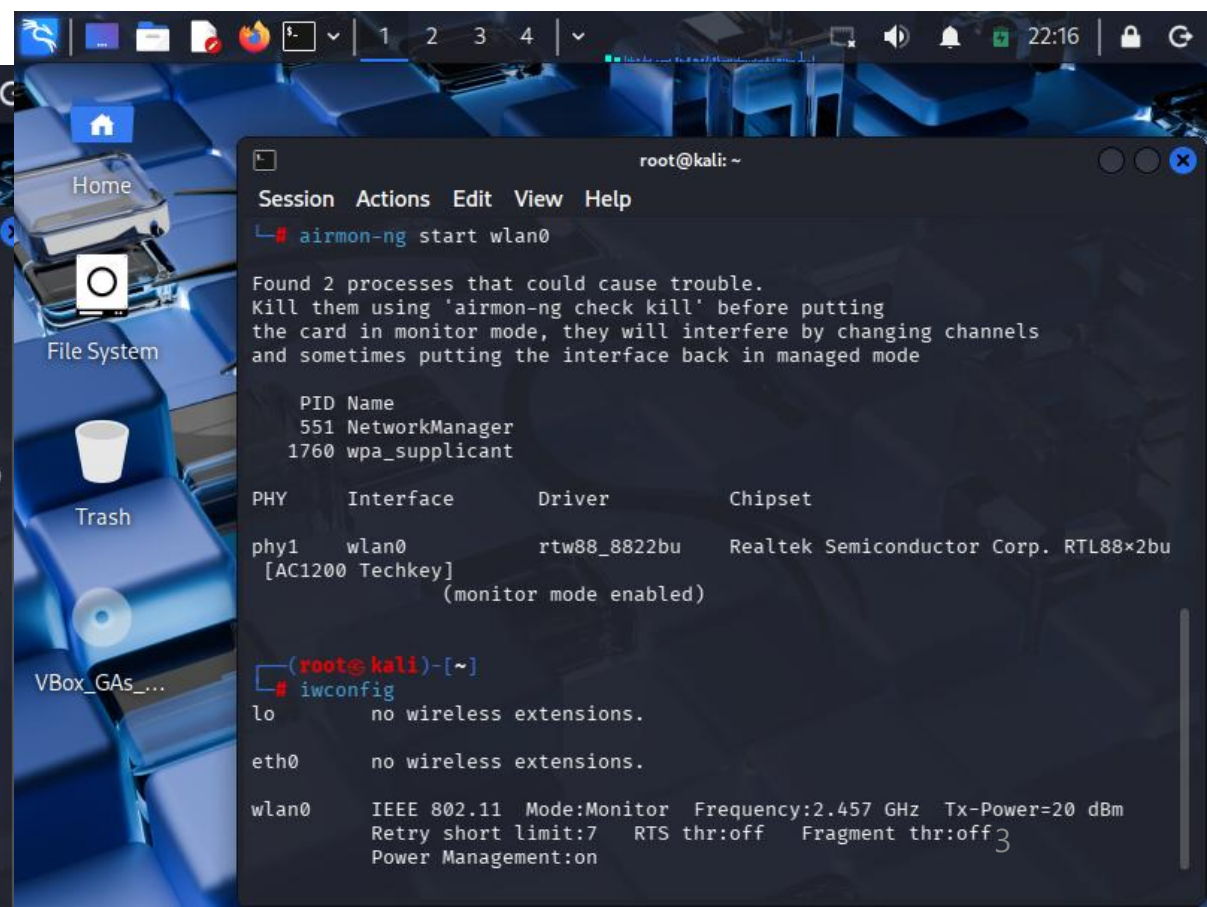
Environment

- OS: Kali linux
- Wireless LAN: ipTIME A3000UA



A terminal window on a Kali Linux desktop. The desktop background is a blue keyboard. Icons for 'Home', 'File System', 'Trash', and 'VBox_GAs_...' are visible. The terminal shows the following commands and output:

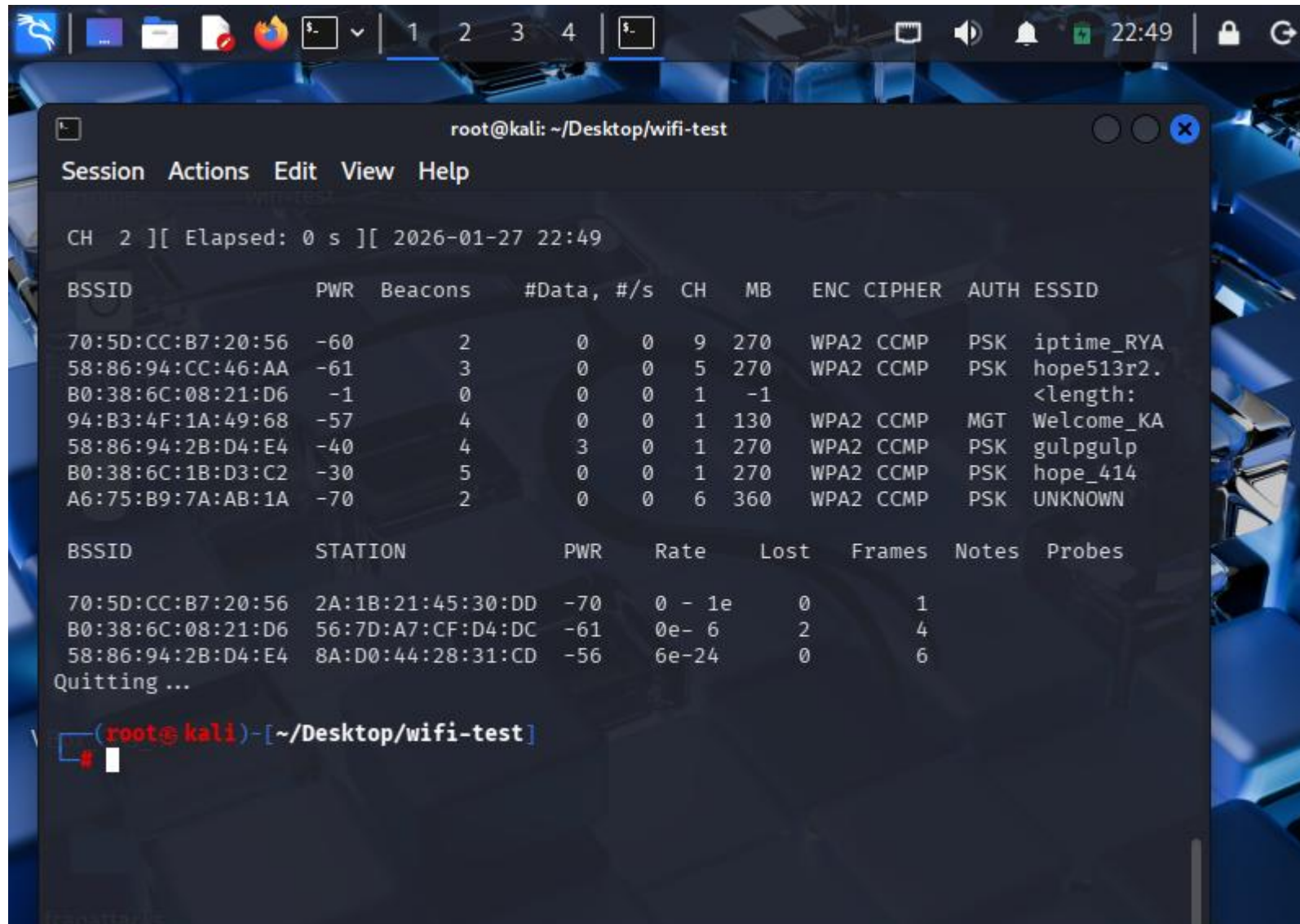
```
root@kali: ~  
Session Actions Edit View Help  
zsh: corrupt history file /root/.zsh_history  
(root@kali)-[~]  
# lsusb  
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub  
Bus 001 Device 002: ID 80ee:0021 VirtualBox USB Tablet  
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub  
Bus 002 Device 002: ID 0bda:b812 Realtek Semiconductor Corp. RTL88x2bu [AC1200 Techkey]  
(root@kali)-[~]  
# iwconfig  
lo        no wireless extensions.  
  
eth0      no wireless extensions.  
  
wlan0     IEEE 802.11  ESSID:off/any  
Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm  
Retry short limit:7  RTS thr:off  Fragment thr:off  
Encryption key:off  
Power Management:on  
(root@kali)-[~]
```



A terminal window on a Kali Linux desktop, showing the output of the 'airmon-ng start wlan0' command. The desktop background is a blue keyboard. Icons for 'Home', 'File System', 'Trash', and 'VBox_GAs_...' are visible. The terminal shows the following commands and output:

```
root@kali: ~  
Session Actions Edit View Help  
# airmon-ng start wlan0  
  
Found 2 processes that could cause trouble.  
Kill them using 'airmon-ng check kill' before putting  
the card in monitor mode, they will interfere by changing channels  
and sometimes putting the interface back in managed mode  
  
PID Name  
551 NetworkManager  
1760 wpa_supplicant  
  
PHY      Interface      Driver      Chipset  
phy1     wlan0          rtw88_8822bu  Realtek Semiconductor Corp. RTL88x2bu  
[AC1200 Techkey]  
          (monitor mode enabled)  
(root@kali)-[~]  
# iwconfig  
lo        no wireless extensions.  
  
eth0      no wireless extensions.  
  
wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm  
Retry short limit:7  RTS thr:off  Fragment thr:off  
Power Management:on
```

Scanning...



```
root@kali: ~/Desktop/wifi-test
Session Actions Edit View Help

CH 2 ][ Elapsed: 0 s ][ 2026-01-27 22:49

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
70:5D:CC:B7:20:56 -60      2         0  0  9  270  WPA2 CCMP PSK iptime_RYA
58:86:94:CC:46:AA -61      3         0  0  5  270  WPA2 CCMP PSK hope513r2.
B0:38:6C:08:21:D6  -1      0         0  0  1  -1    WPA2 CCMP PSK <length:
94:B3:4F:1A:49:68 -57      4         0  0  1  130  WPA2 CCMP MGT Welcome_KA
58:86:94:2B:D4:E4 -40      4         3  0  1  270  WPA2 CCMP PSK gulpgulp
B0:38:6C:1B:D3:C2 -30      5         0  0  1  270  WPA2 CCMP PSK hope_414
A6:75:B9:7A:AB:1A -70      2         0  0  6  360  WPA2 CCMP PSK UNKNOWN

BSSID          STATION          PWR   Rate    Lost  Frames  Notes  Probes
70:5D:CC:B7:20:56 2A:1B:21:45:30:DD -70    0 - 1e    0      1
B0:38:6C:08:21:D6 56:7D:A7:CF:D4:DC -61    0e- 6    2      4
58:86:94:2B:D4:E4 8A:D0:44:28:31:CD -56    6e-24    0      6
Quitting ...

(root@kali)-[~/Desktop/wifi-test]
```

Utilization (example)

- Connecting WLAN card with Kali linux
- Run with monitor mode
- Scan wifi packets with airodump-ng command
- Capture 4-way Handshake with aireplay-ng command
 - (Deauth: aireplay-ng -deauth [num] -a [MAC addr] wlan0)
- Dictionary attack with Aircrack-ng command

PMKID offline dictionary attack

- Client-less attack
 - Attacker receives EAPOL Message 1 from AP
 - Dictionary attack can be possible for PMKID in M1

The screenshot displays two windows from a Kali Linux desktop. The left window is a terminal running the `hcxdump` tool to capture EAPOL messages from a wireless interface. The right window is Wireshark, showing a packet capture of the captured data, with a focus on EAPOL messages.

Terminal Window:

```
root@kali: ~/Desktop/wifi-test
Session Actions Edit View Help
(root@kali)-[~/Desktop/wifi-test]
# sudo hcxdump -i wlan0 -w hotspot_capture.pcapng

This is a highly experimental penetration testing tool!
It is made to detect vulnerabilities in your NETWORK mercilessly!
Misuse within a network, without specific authorization, may cause
irreparable damage and result in significant consequences!
Not understanding what you were doing is not going to work as an excuse!

BPF is unset! Make sure hcxdump is running in a 100% controlled environment!

starting ...
^C
13195 Packet(s) captured by kernel
0 Packet(s) dropped by kernel
exit on sigterm

(root@kali)-[~/Desktop/wifi-test]
```

Wireshark Window:

The Wireshark window shows a packet capture of the data. The packet list pane on the left shows several EAPOL messages. The packet details pane on the right shows the structure of an EAPOL message, including the EAP code, EAP ID, and EAP payload. The packet bytes pane at the bottom shows the raw data of the captured packets.

Packet No.	Time	Source	Destination	EAPOL Message
1	0.000000	192.168.1.1	192.168.1.2	REASSOCIATIONREQUEST (PSK)
2	0.000000	192.168.1.1	192.168.1.2	EAP (total)
3	0.000000	192.168.1.1	192.168.1.2	EAP CODE request
4	0.000000	192.168.1.1	192.168.1.2	EAP CODE response
5	0.000000	192.168.1.1	192.168.1.2	EAP ID
6	0.000000	192.168.1.1	192.168.1.2	EAP-PEAP
7	0.000000	192.168.1.1	192.168.1.2	EAPOL messages (total)
8	0.000000	192.168.1.1	192.168.1.2	EAPOL RSN messages
9	0.000000	192.168.1.1	192.168.1.2	EAPOLTIME gap (measured maximum msec)
10	0.000000	192.168.1.1	192.168.1.2	EAPOL ANONCE error corrections (NC)
11	0.000000	192.168.1.1	192.168.1.2	REPLAYCOUNT gap (suggested NC)
12	0.000000	192.168.1.1	192.168.1.2	EAPOL M1 messages (total)
13	0.000000	192.168.1.1	192.168.1.2	EAPOL M2 messages (total)
14	0.000000	192.168.1.1	192.168.1.2	EAPOL M3 messages (total)
15	0.000000	192.168.1.1	192.168.1.2	EAPOL M4 messages (total)
16	0.000000	192.168.1.1	192.168.1.2	EAPOL M4 messages (zeroed NONCE)
17	0.000000	192.168.1.1	192.168.1.2	EAPOL pairs (total)
18	0.000000	192.168.1.1	192.168.1.2	EAPOL pairs (host)

Dictionary attack

[illegible]

The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window is open, displaying the output of a hashcat session. The session has reached a 'Warning: Approaching final keyspace - workload adjusted.' status. The terminal shows the following details:

- Session: hashcat
- Status: Exhausted
- Hash.Mode: 22000 (WPA-PBKDF2-PMKID+EAPOL)
- Hash.Target: hotspot_pmkid.hashcat
- Time.Started: Wed Jan 28 00:16:41 2026 (0 secs)
- Time.Estimated: Wed Jan 28 00:16:41 2026 (0 secs)
- Kernel.Feature: Pure Kernel (password length 8-63 bytes)
- Guess.Base: File (test_pwd.txt)
- Guess.Queue: 1/1 (100.00%)
- Speed.#01: 2145 H/s (0.55ms) @ Accel:187 Loops:1024 Thr:1 Vec:8
- Recovered: 0/5 (0.00%) Digests (total), 0/5 (0.00%) Digests (new), 0/4 (0.00%) Salts
- Progress: 24/24 (100.00%)
- Rejected: 0/24 (0.00%)
- Restore.Point: 6/6 (100.00%)
- Restore.Sub.#01: Salt:3 Amplifier:0-1 Iteration:1-3
- Candidate.Engine: Device Generator
- Candidates.#01: 12345678 → password123
- Hardware.Mon.#01: Util: 39%

The terminal also shows the session started on Wed Jan 28 00:16:39 2026 and stopped on Wed Jan 28 00:16:43 2026. In the background, a Firefox ESR window is open, displaying the title 'Browse the World Wide Web' and the address bar showing 'root@kali: ~/Desktop/wifi-test'. The desktop background is a dark, abstract image.

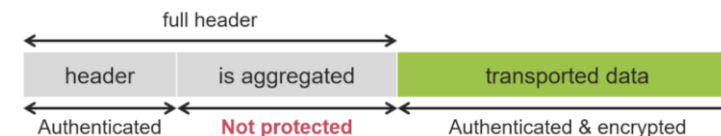
KRACK

- MitM attack
 - Key installation by resending Message 3
 - Utilize same key (parameters get reset when reinstalled)
- Packets can be replayed, decrypted, and/or forged which causes
 - Bypassing HTTPS
 - Intercept important information
- <https://youtu.be/Oh4WURZoR98>

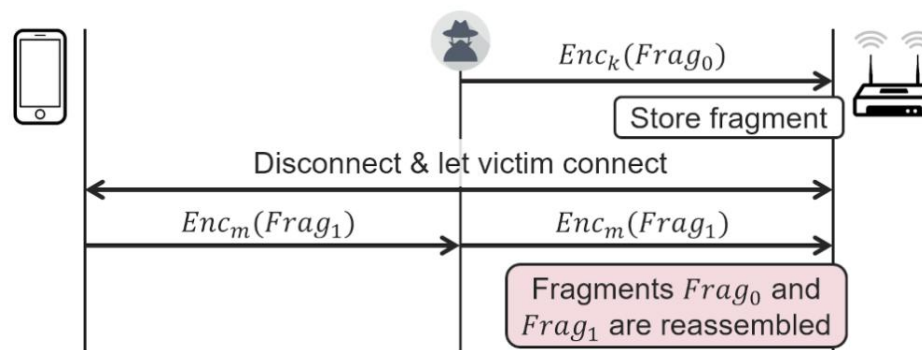
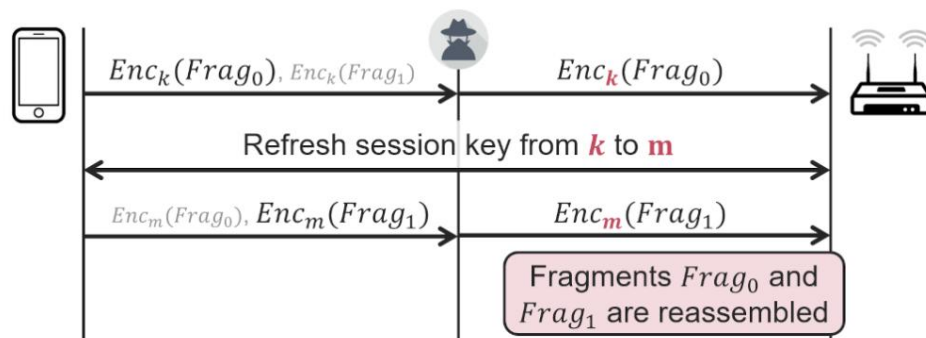
Vulnerability check (KRACK)

- [vanhoefm/krackattacks-scripts](https://github.com/vanhoefm/krackattacks-scripts)
 - It creates virtual AP on device. It can test its connected client by resending M3s in different situations

Fragattacks



- Injecting unencrypted wi-fi frame
 - Aggregation attack → fixed by “is aggregated” flag
 - Mixed key attack can use reassemble fragments that were decrypted by different keys → more likely a theoretical attack
 - Fragment cache attack can send malicious fragment that can be combined within the other fragments → fixed by removing fragments when disconnection or (re)connection
- [FragAttacks: Breaking Wi-Fi through Fragmentation and Aggregation](#)



Vulnerability check (Fragattacks)

- [vanhoefm/fragattacks](https://vanhoefm.github.io/fragattacks/)
 - Check by sending various fragmented pings to devices in different conditions.

Reference

- [New attack on WPA/WPA2 using PMKID](#)
- [ccs2017.pdf](#) ([KRACK Attacks: Breaking WPA2](#))
 - [vanhoefm/krackattacks-scripts](#)
- [usenix2021.pdf](#) ([FragAttacks: Security flaws in all Wi-Fi devices](#))
 - [vanhoefm/fragattacks](#)