WPA2 útoky + KRACK

(prezentace do PVBPS)

Richard Zavadil

28.11.2017

Obsah

- Wi-Fi standard + WPA2 úvod
- Autentizace, asociace
- WPA2
- 4-way handshake
- Útoky na WPA2-PSK
- KRACK

Wi-Fi + WPA2

- Dnes nejrozšířenější způsob zabezpečení (58%)
- **Personal** / Enterprise
- SSID, heslo
- Pasivní skenování
  - AP posílá Beacon frames

No.	Time	Source	Destination	Protocol	Length	Info
13	0.235105	AsustekC_4e:06:1d	Broadcast	802.11	248	Beacon frame, SN=563, FN=0, Flags=........C, BI=100, SSID=root_wpa2
16	0.265969	ZyxelCom_af:4e:00	Broadcast	802.11	335	Beacon frame, SN=938, FN=0, Flags=........C, BI=100, SSID=DerSchal
17	0.309413	UbeeInte_54:33:e0	Broadcast	802.11	318	Beacon frame, SN=855, FN=0, Flags=........C, BI=100, SSID=Monika
19	0.337531	AsustekC_4e:06:1d	Broadcast	802.11	248	Beacon frame, SN=565, FN=0, Flags=........C, BI=100, SSID=root_wpa2
22	0.368362	ZyxelCom_af:4e:00	Broadcast	802.11	335	Beacon frame, SN=939, FN=0, Flags=........C, BI=100, SSID=DerSchal
23	0.395720	CompalBr_ea:7c:79	Broadcast	802.11	353	Beacon frame, SN=1926, FN=0, Flags=........C, BI=100, SSID=UPC9DB6BF5
24	0.409332	UbeeInte_a3:d0:21	Broadcast	802.11	322	Beacon frame, SN=2853, FN=0, Flags=........C, BI=100, SSID=UPC5705026
26	0.439864	AsustekC_4e:06:1d	Broadcast	802.11	248	Beacon frame, SN=567, FN=0, Flags=........C, BI=100, SSID=root_wpa2
30	0.470777	ZyxelCom_af:4e:00	Broadcast	802.11	335	Beacon frame, SN=940, FN=0, Flags=........C, BI=100, SSID=DerSchal
31	0.498406	CompalBr_ea:7c:79	Broadcast	802.11	353	Beacon frame, SN=1927, FN=0, Flags=........C, BI=100, SSID=UPC9DB6BF5
32	0.511740	UbeeInte_a3:d0:21	Broadcast	802.11	322	Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID=UPC5705026

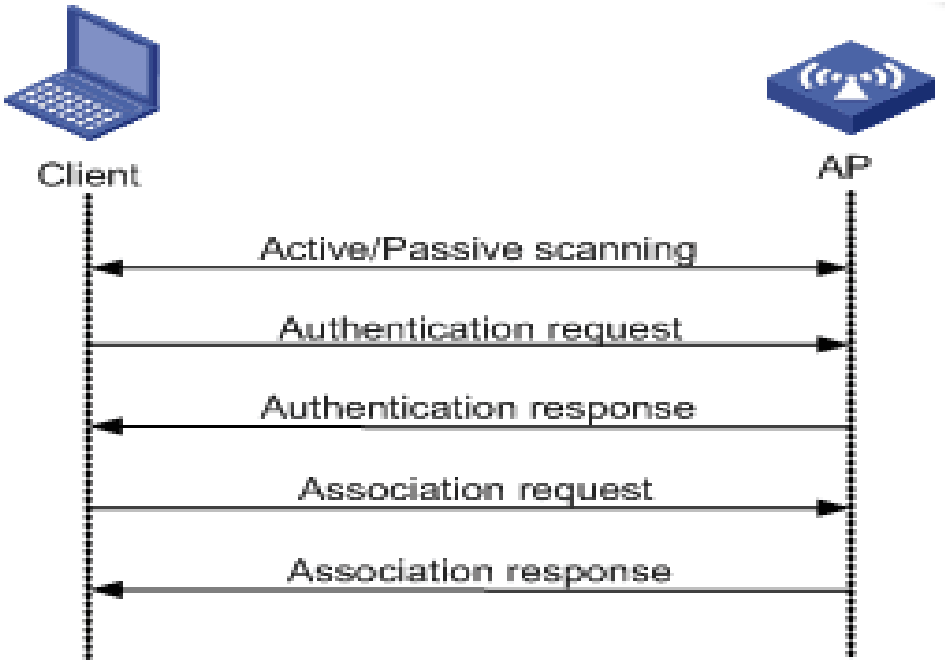
IEEE 802.11

- Aktivní skenování
  - Probe request (na broadcast), probe response
  - Může se ptát na specifickou síť

No.	Time	Source	Destination	Protocol	Lengtl	Info
128	1.003381000	EdimaxTe_27:b6:d9	Broadcast	802.11	117	Probe Request, SN=1975, FN=0, Flags=........C, SSID=Mikulda
763	7.368639000	00:6d:52:36:b5:ce	Broadcast	802.11	197	Probe Request, SN=1905, FN=0, Flags=........C, SSID=CADJ
2250	23.10009200(	IntelCor_b0:d2:9a	Broadcast	802.11	121	Probe Request, SN=281, FN=0, Flags=........C, SSID=upcbauerovi
2601	26.85192700(	e8:15:0e:a9:c5:39	Broadcast	802.11	116	Probe Request, SN=2687, FN=0, Flags=........C, SSID=OLIVER
2602	26.85287400(	e8:15:0e:a9:c5:39	Broadcast	802.11	121	Probe Request, SN=2688, FN=0, Flags=........C, SSID=KingdomHall

Autentizace, asociace Wi-Fi

- Authentication request
  - MAC + zjištění autentizačního algoritmu
- Association request
  - Alokace prostředků na AP. AID, rychlost, šifrování…

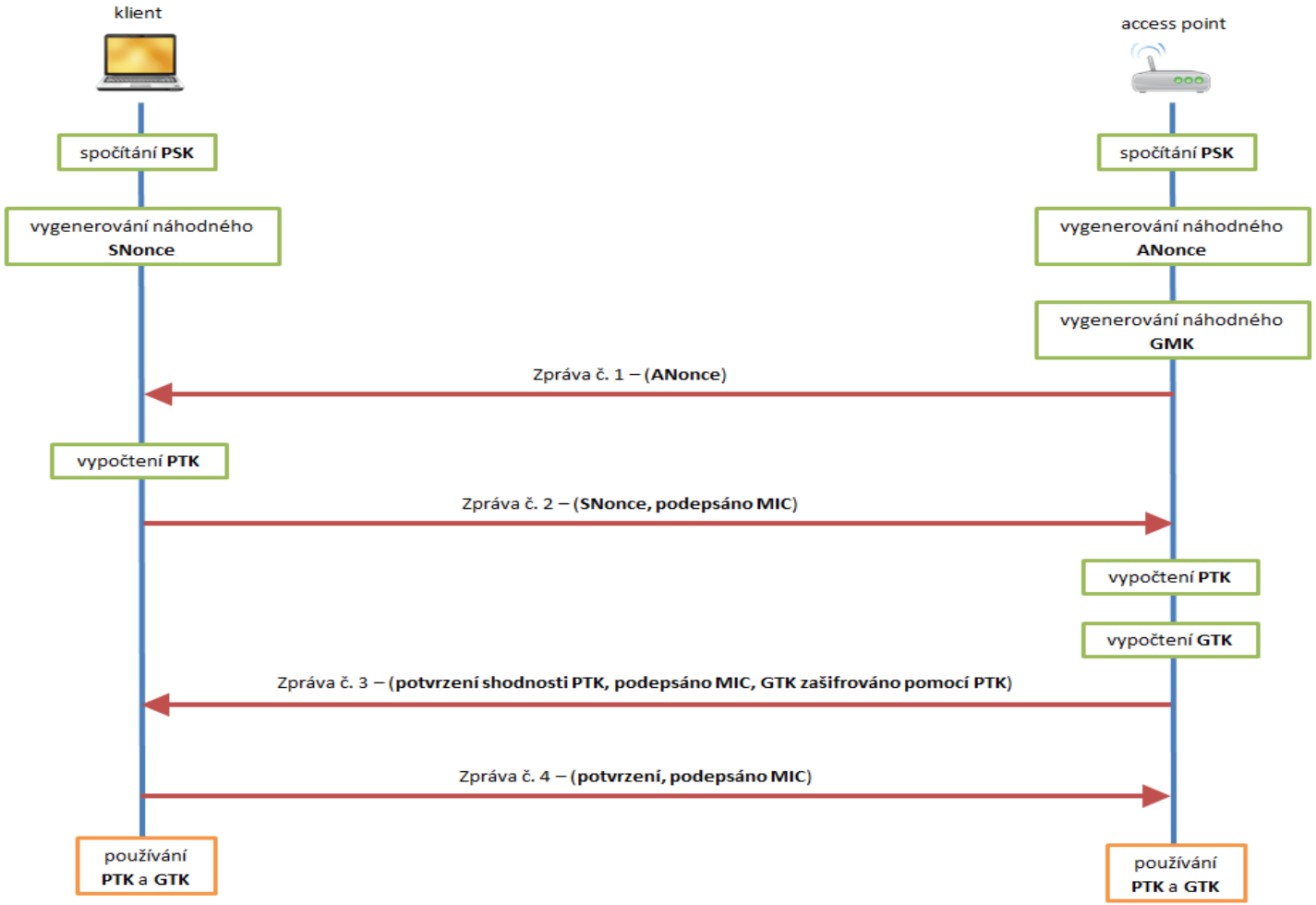


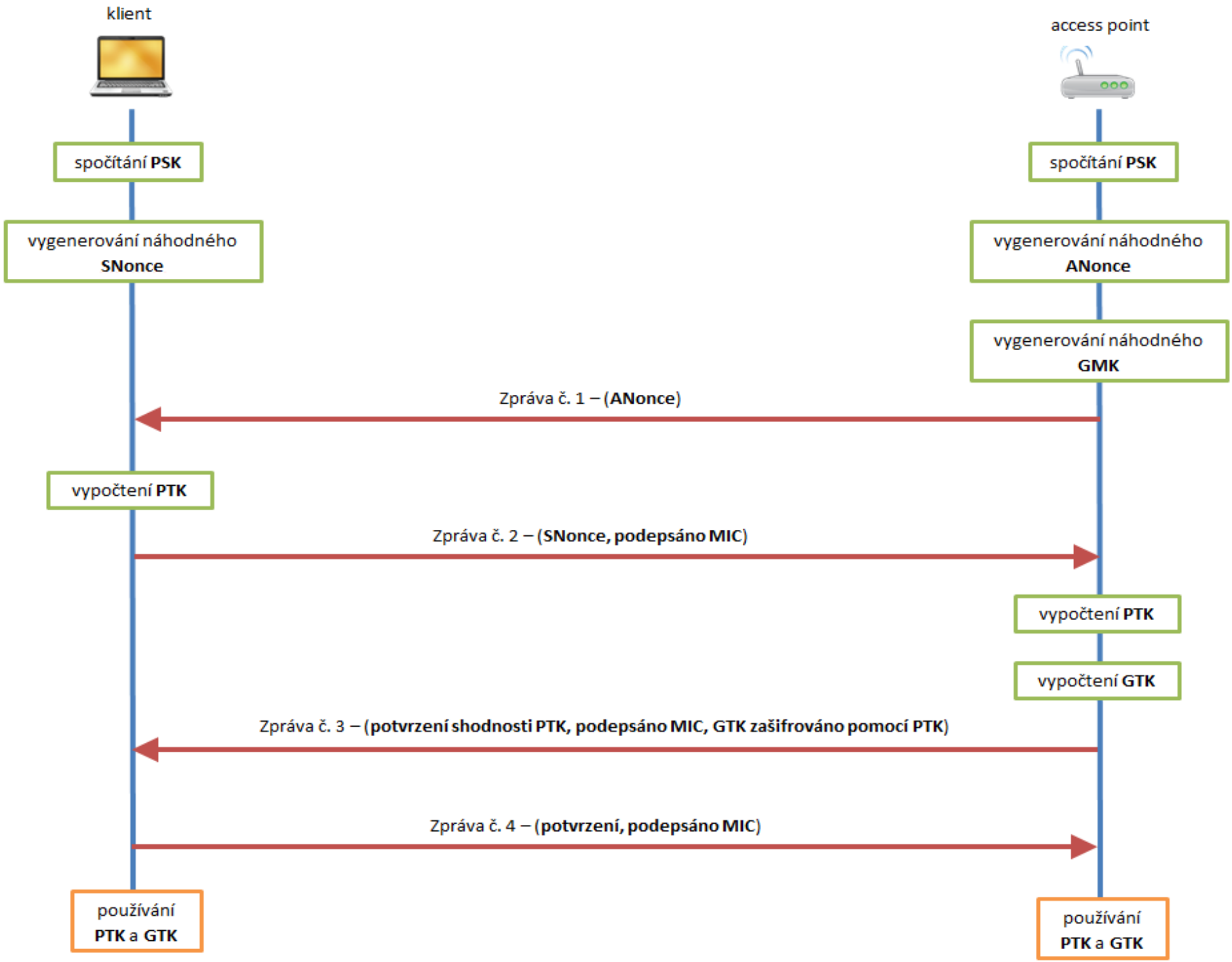
WPA2 - PSK

- **W**i-Fi **P**rotected **A**ccess
- WPA2-PSK-CCMP
  - AES využívající vygenerovaných kličů
- Pre-shared key
- SSID, heslo
- PSK = PBKDF2 (HMAC-SHA1, **heslo**, **SSID**, 4096, 256)
- Klient i AP samostatně
- PTK, GTK <- GMK

4-way handshake

- AP a klient se dohodnou na šifrovacích klíčích
- PSK
- ANonce
- SNonce
- 2xMAC
- MIC
- PRF-384




klient
access point
spočítání PSK
spočítání PSK
vygenerování náhodného SNonce
vygenerování náhodného ANonce
vygenerování náhodného GMK
Zpráva č. 1 – (ANonce)
vypočtení PTK
Zpráva č. 2 – (SNonce, podepsáno MIC)
vypočtení PTK
vypočtení GTK
Zpráva č. 3 – (potvrzení shodnosti PTK, podepsáno MIC, GTK zašifrováno pomocí PTK)
Zpráva č. 4 – (potvrzení, podepsáno MIC)
používání PTK a GTK
používání PTK a GTK

Útoky na WPA2-PSK

- **Slovníkový útok**
- **Upravený slovníkový útok**
  - Online zachycení:
    - **ANonce**, **SNonce**, **MIC**
  - Offline výpočet:
    - **PSK** pomocí PBKDF2 <- heslo ze slovníku
    - **PTK** pomocí PRF-384
    - Vypočítání **MIC** a srovnání se zachyceným

Útoky na WPA2-PSK

- **WPS útok**
  - Wifi protected setup (PIN, NFC, USB, fyzicky)
  - Nemusí být aktivní na AP
  - 8 místné číslo (**10^8 kombinací** (3 sec na pokus)
  - 4 + 3 + 1 (4^10 + 3^10 = **11k kombinací**)
  - Obrana
    - Vypnout WPS, update firmware
- Social engineering
- Dešifrování provozu v síti

KRACK

- **K**ey **R**einstallation **A**tta**ck**s
- Chyba protokolu -> zranitelnost všech zařízení
- Organizace patchují firmware
- Nezjišťuje heslo
- 4-way handshake

KRACK průběh

- Vytvoření rogue AP (manipulace s handshakem)
- Připojení klienta k AP (MitM rogue AP)
- Podstrčení vlastního šifrovacího klíče

KRACK ukázka

- https://www.youtube.com/watch?v=Oh4WURZoR98

Zdroje

- https://www.wireshark.org/tools/wpa-psk.html
- https://www.root.cz/clanky/odposlouchavani-a-prolamovani-wi-fi-siti-zabezpecenych-pomoci-wpa2/
- http://www.mrpear.net/cz/blog/386/prolomeni-wpa-wpa2-psk-pres-wps-snadno-a-rychle-teorie
- https://www.krackattacks.com/
- https://en.wikipedia.org/wiki/KRACK
- https://www.root.cz/clanky/sifrovani-wpa2-bylo-prolomeno-wi-fi-site-je-mozne-odposlouchavat/