Ondřej Václavek
Software engineer, HAVIT, s.r.o.
vaclavek@havit.cz

Wi-Fi security - part II.
WPA / WPA2 / WPA 3

Agenda

- V prvním díle:
  - Obecný úvod, legislativa
  - Co je Wi-Fi a jak to funguje?
  - Šifrování Wi-Fi sítí
  - Co je WEP?
- Co je WPA / WPA2 a WPA3?
- Co je WPS
- Možné útoky
- Praktické ukázky

Šifrování Wi-Fi sítí

- WEP – požívá šifrování RC4
- WEPplus – nastavba WEP, odstraňuje slabé IV
  - Musí jej podporovat všechny strany, aby byl využit
- WPA – interně používá WEP, slabiny odstraněny protokolem TKIP místo RC4
  - „rychlé odstranění nedostatků děravého WEP na stávající zařízení“
- WPA2 – nově šifrování AES-CCMP
  - Nestačí „update firmware“
- WPA3 – nově 128 bit key, „Dragonfly handshake“
  - Nestačí „update firmware“
- Enterprise autorizace s 802.11X využívá autentizační server, např. RADIUS
  - Multiple schemes - PEAP (username + pass), EAP-TLS (certificates), EAP-SIM (mobiles), LEAP (Cisco) …

Co je WPA

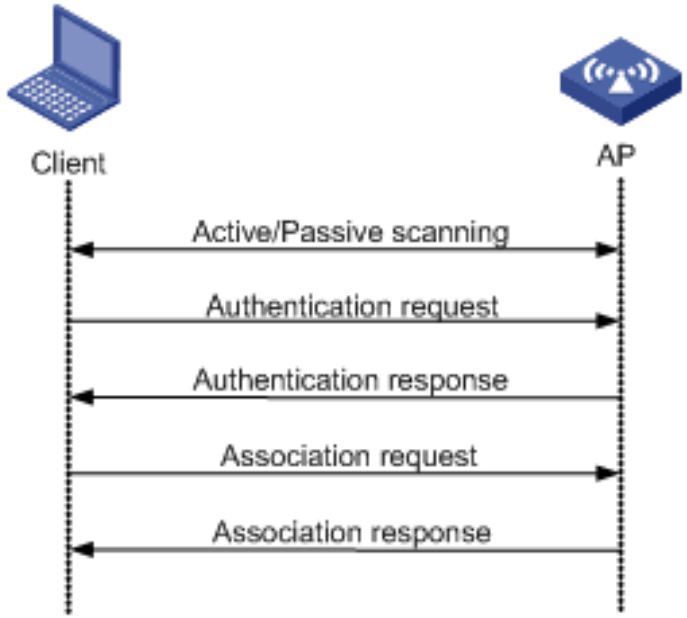
- Rychlá náhrada za prolomený WEP
- Řeší generování slabých IV pomocí nového protokolu TKIP
- Lepší kontrola integrity dat (nefunkční útoky s poškozenými rámci)
- Algoritmus Michael bránící útokům opakováním rámců (obsahuje počítadlo rámců)
- … dnes obsolete, možné využití v „kompatibilních“ mixed zabezpečeních

Slabiny WPA

- Rainbow tabulky pro obvyklá SSID a hesla
- Chybí „Forward secrecy“ – pokud se někdy k síti podaří prolomit heslo, je možné dešifrovat veškerou zachycenou komunikaci
- Úspěšné útoky na broadcast packety
- Úspěšné útoky s injektováním malých dat (port scanning, JS injections)
- WPS

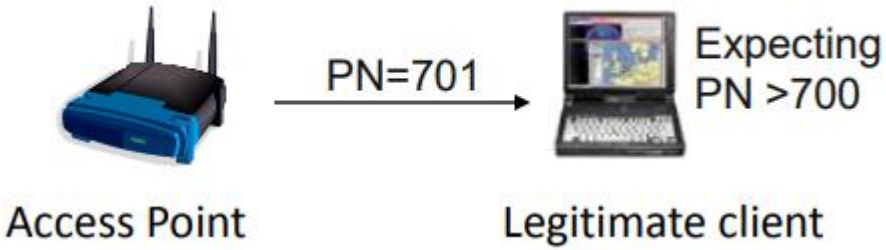
Co je WPA2

- Vylepšení WPA, přidává k TKIP algoritmus CCMP založený na blokové šifře AES
- Od 2004 povinná, aby zařízení mohlo být „Wi-Fi“
- 4-way handshake: PSK spočítaný na základě SSID a hesla
  - PTK (pairwise temp. key) pro unicast
  - GTK (group key) pro multicast



Slabiny WPA2

- Rainbow tabulky pro obvyklá SSID a hesla (PSK)
- Insider útoky pomocí GTK (útok Hole196)
  - Traffic snooping, MITM, TCP resets, port scanning, fram
- Chybí „Forward secrecy“
- Packet Number in CCMP
- WPA2 Radius s MS-CHAPv2 prolomeno
- Slabý RNG -> odhadnutelný GTK
- KRACK attack (08/2017), zranitelné některé implementace (replay attack)
- WPS



Co je WPA3

- Nový standard zabezpečení Wi-Fi sítí z roku 2018
- Náhrada PSK za SAE založené na teorii konečných cyklických grup a eliptických křivkách
- V SAE také MAC adresy AP i klienta (ochrana proti rainbow tabulkám)
- Forward secrecy
- Ochrana management frames (ochrana proti deauth) dle IEEE 802.11w
- Enterprise mód WPA3-CNSA (Commercial National Security Agency)
- Náhrada WPS pomocí registrace veřejného klíče do wifi (QR kód IoT zařízení)

Slabiny WPA3

- Dragonblood attack (04/2019) – útok na implementace
  - Downgrade attacks
  - Side-channel attacks -> brute force
  - DOS

WPS

- Wi-Fi Protected Setup (původně Wi-Fi Simple Config)
- Představeno 2006 (Cisco)
- Prolomeno 12/2011, od 2014 řádově minuty
- Módy
  - PIN 8 znaků
  - Push button
  - NFC
  - USB data transfer (deprecated)

Slabiny WPS

- „Online“ brute-force attack (2011) pro 10^7 kombinací ~ 10 000 000 ~ 11 dnů
- Špatný návrh protokolu = špatně znak v první/druhé polovině ~ 11 000 < 4h
- Pixie-dust attack (2014) – nedostatečný RND ~ 5 minut
- PIN často nelze změnit. Nijak
- Fyzický přístup k zařízení
- Z PINu lze odvodit PSK

Praktické ukázky

Síť hackme

- AP TP-Link
- WPA2 PSK
- WPS zapnuté
- heslo: tajneheslo
- Vektor útoku:
  - Počkáme na připojení klienta
  - Deauth packet
  - Odchytíme nový handshake
  - Hádáme heslo dle slovníku

Síť hackmeWPA2

- AP Huawei CPE B593 (starý)
- WPA2 PSK
- WPS zapnuté
- Vektor útoku:
  - Útočíme na zranitelné WPS
  - Brute-force
  - Ochrana routeru – zamykání PINU na 3 minuty po 3 neúspěšných pokusech.
  - 11000 možností ~ 7 dnů

Síť hackmeWPA

- AP Huawei B310s (nový)
- WPA2 PSK
- WPS vypnuté
- Vektor útoku:
  - Naslouchámе a ukládáme data
  - Čekáme na libovolný EAPOL frame
  - Handshake uložíme
  - Převedeme do formátu, kterému rozumí hashcat
  - Distribuovaně hádáme heslo (vč. podpory grafických karet)
  - Nedetekovatelný útok (nevysíláme) …

Distribuované „služby“

- https://gpuhash.me/
- https://project-rainbowcrack.com/table.htm

V příštím díle …

- Dešifrování provozu
- Únosy spojení
- MITM
- SSL Stripping
- … ☺