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

Wi-Fi security - part I.

WEP

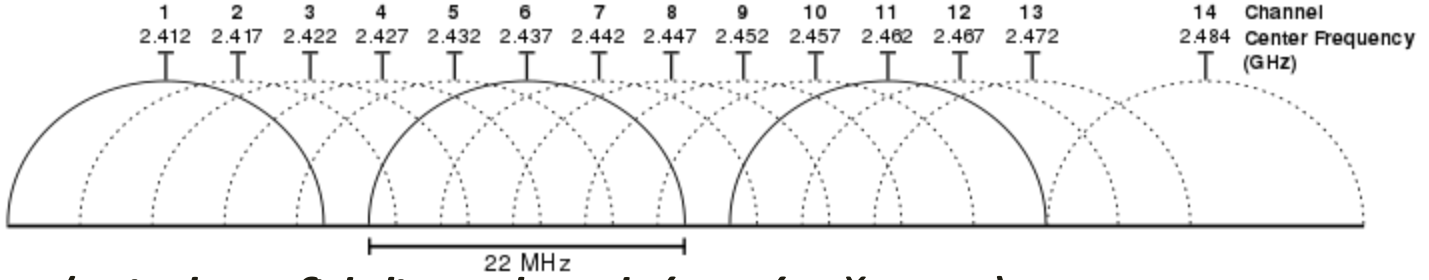
Agenda

- Legislativa
- Co je Wi-Fi a jak to funguje?
- Šifrování Wi-Fi sítí
- Co je WEP?
- Jak to funguje
- Možné útoky
- Praktická ukázka

Legislativa

- Zákon č. 40/2009 Sb., trestní zákoník
- § 230
- **(1)** Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na **dvě léta**
- **(3)** Odnětím svobody na **šest měsíců až čtyři léta** … bude pachatel potrestán … v úmyslu způsobit jinému škodu nebo újmu nebo … omezit funkčnost počítačového systému …
- **(4)** Odnětím svobody na **jeden rok až pět let** … spáchá-li čin …jako člen organizované skupiny
- **(5)** Odnětím svobody na **tři léta až osm let** … způsobí-li činem … škodu velkého rozsahu

Co je Wi-Fi



- Wi-Fi = bezvýznamová zkratka, (*wireless fidelity = bezdrátová věrnost)*
- 1962 děrný štítek přenesen „vzduchem“ rozprostřeným radiovým spektrem
- V 80. letech uvolněno pro civilní použití
- 1997 standardizováno normou IEEE 802.11, stále se vyvíjí. Aktuální 802.11ax
- 13 kanálů po 5 MHz (+1 Japonsko) ve bezlicenčním pásmu 2,4 GHz a 5 GHz
- V různých zemích povolené různé frekvence
- Nepovolený výkon / frekvence kontroluje ČTU
  - zákon č. 127/2015 Sb., o elektronických komunikacích, §22 – pokuty 100 tis Kč - 20 mio Kč.

Jak funguje Wi-Fi

- Každý Access Point (i peer) broadcastuje beacon frame (obvykle 10 – 100x za sekundu)
  - Textový identifikátor SSID - „název“
  - V rámci je MAC adresa AP – standartní linková vrstva
  - Compatibility info (šifrování, typ sítě adhoc/infrastructure)
  - Podporované rychlosti
  - Timestamp
  - Další pro nás momentálně nezajímavé informace

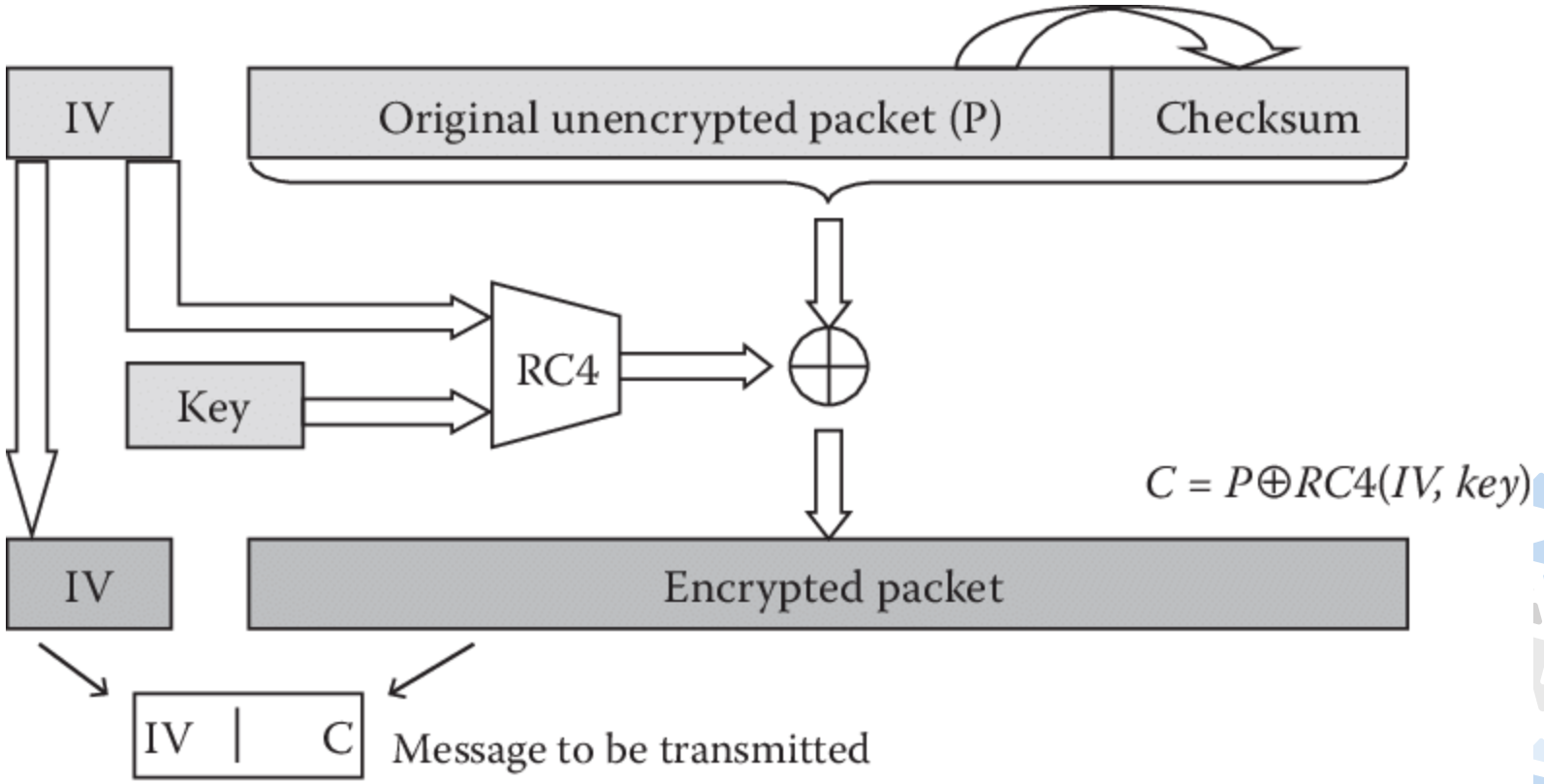
Šifrování Wi-Fi sítí

- 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 WEP

- WEP = Wired Equivalent Privacy (1997 – 2003)
- 64 bit / 128 bit / (256 bit) šifrování
  - 24 bit **initialization vector** (IV) + 10 / 26 **shared hexadecimal key** (24 + 10 * 4, 24 + 26 * 4)
- RC4 **stream** cipher + CRC32
- IV jako prevence opakování stejných klíčů
  - Jejich ale málo, takže v 5000 paketech je 50% pravděpodobnost stejného IV
  - Toho využívá Related key attack
- Open system authentication - připojit se může každý, šifrují se data
- Shared key authentication – autentizace klíčem (challenge - response)

Jak vypadá WEP šifrování



Možné základní útoky (a další)

- Fluhrer-Mantin-Shamir attack
  - útok na slabé IV u RC4 šifrování. Slabé IV „špatně“ šifrují část rámců. Ze slabých IV „statisticky“ odvodíme klíč
  - 64bit = 0,0198% of weak seeds, 128bit = 0,0565% of weak seeds
- KoreK chopchop attack
  - U známého packetu měníme jednotlivé bity, dopočítáme CRC a posíláme na AP. Pokud AP odpoví, packet byl správný -> známe bit rámce. Opakujeme až dešifrujeme celý rámec (a RC4 proud pro IV).
- Fragmentation attack
  - Vytvoříme malé fragmentované rámce, sašifrujeme známým IV a pošleme na AP. Ten je defragmentuje do velikosti MTU, zašifruje a rozešle klientům. Známe obsah => můžeme dešifrovat
- Cafe-latte attack
  - Generování rámců - Oddchytíme ARP packet od oběti, modifikujeme bit a pošleme zpět. On nám odpoví ARP packetem, že tam máme chybu. A pořád dokola.

Praktická ukázka

Pass: **Ux@4J3wgQ!m9K**