Zabezpečení Wi-Fi sítí

Ondřej Caletka

1. března 2012

Obsah

Bezpečnost infrastruktury

Zajištění před nežádoucím připojením:

- šifrování
- regulace přístupu na vyšší vrstvě
- ostatní neúčinné metody
  - skrytí ESSID (lze snadno odkrýt)
  - seznam povolených MAC adres (lze zfalšovat)

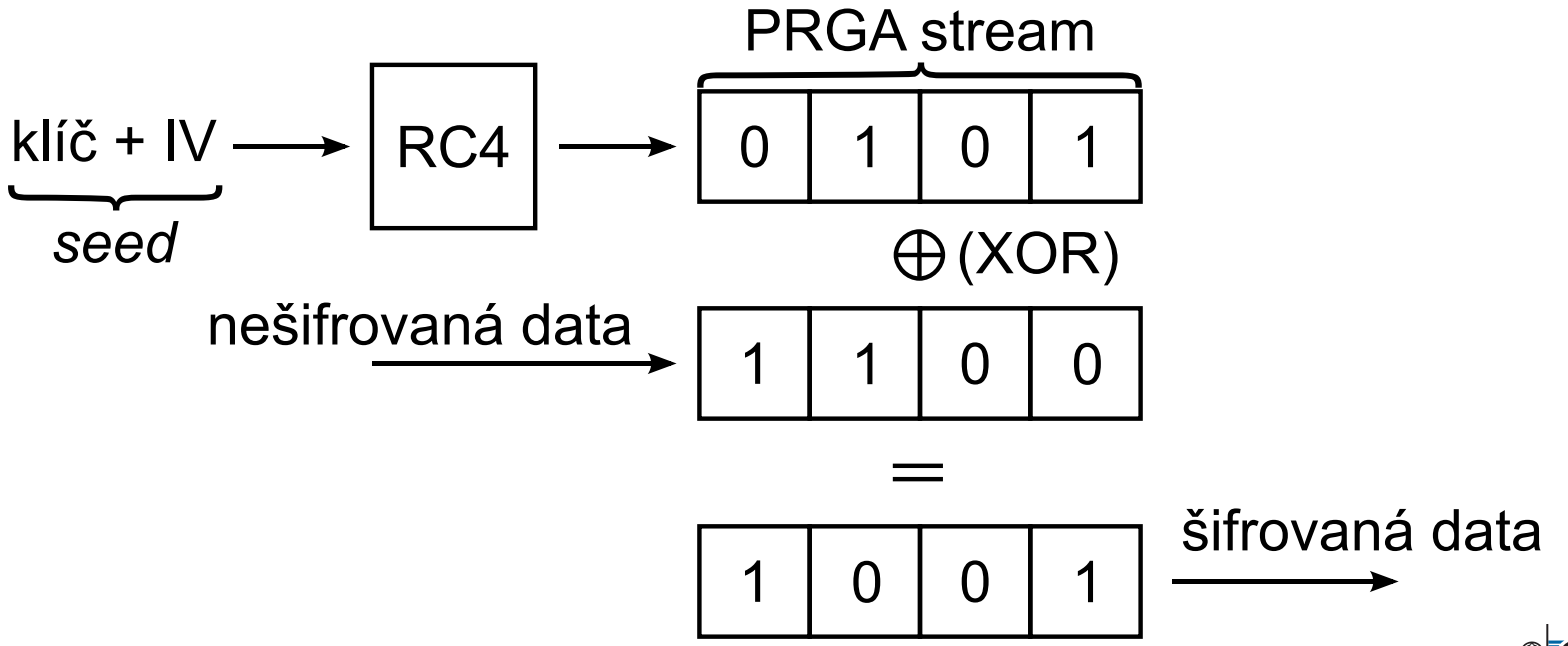
Šifrování

- Wired Equivalent Privacy
  - vytvořen 1999, prolomen 2001
  - symetrická šifra se sdíleným klíčem
- Wi-Fi Protected Access
  - vytvořen 2002, zavržený od roku 2009
  - HW kompatibilní s WEP
- Wi-Fi Protected Access 2
  - vytvořen 2004, povinná podpora od 2006
  - nový protokol CCMP, založený na AES
  - zatím bez známých slabých míst

CESNET

Wired Equivalent Privacy

- proudová šifra RC4
- klíč délky 64-bitů
  - po roce 2000 - klíče 128 a 256 bitů
  - 24 bitů z klíče tvoří inicializační vektor, proměnný pro každý rámec



Slabá místa WEP

- opakování IV po 2^{24} rámcích
  $\Longrightarrow$ opakování PRGA sekvence
- nenáhodný obsah začátku nešifrovaných dat

Začátek každého rámce s IPv4

0xAA	0xAA	0x03	0x00	0x00	0x00	0x08	0x00
DSAP	SSAP	CTRL	ORG code			ether type	

- možnost fragmentace na úrovni rámců
- autentizace sdíleným klíčem

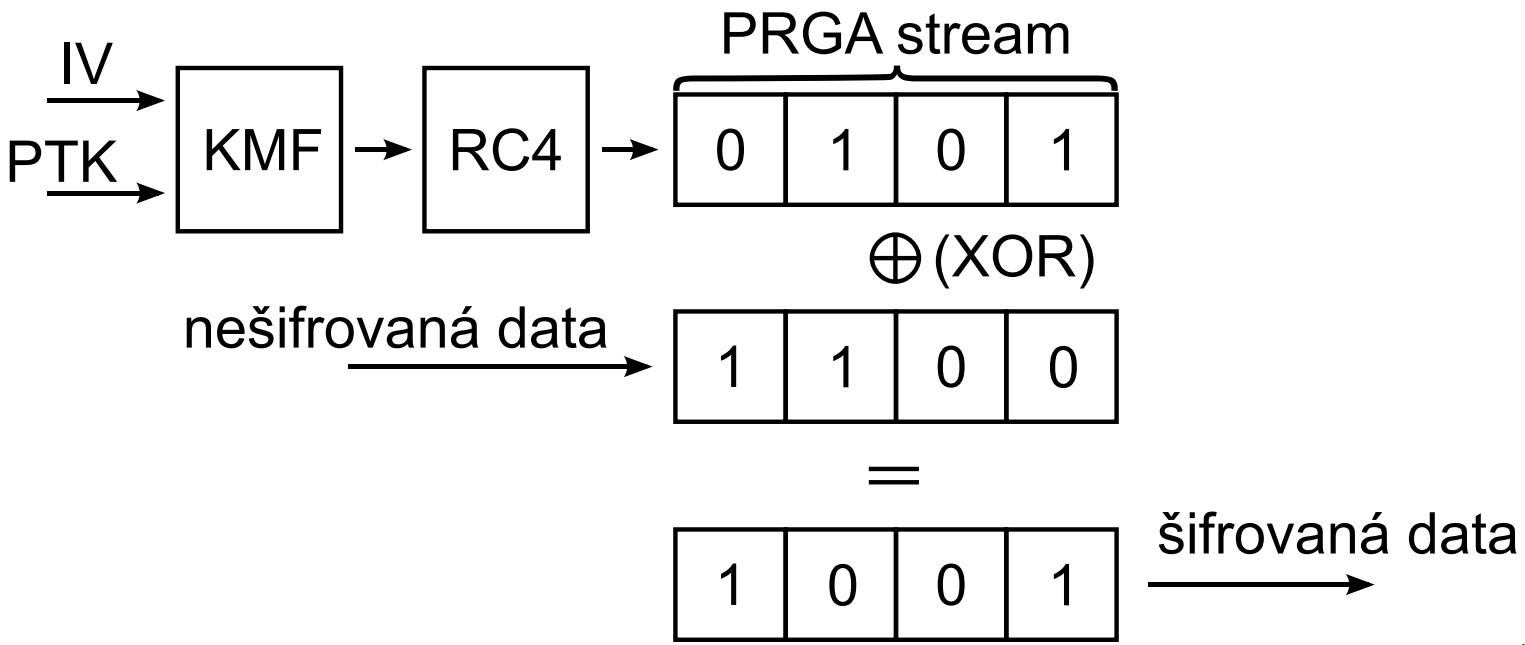
Hlavní útoky na WEP

- zjištění WEP klíče – `aircrack-ng`
  - IV se přenášejí otevřeně
  - je možné zjistit začátek PRGA sekvence
  - po zachycení cca. 500 000 kombinací

- injekce dat – `airreplay-ng`
  - známá dvojice IV + část PRGA, fragmentace
  - broadcast rámec $\rightarrow$ AP jej zopakuje s jiným IV
  - umělé vyvolání nových IV pro zjištění WEP klíče

Wi-Fi Protected Access

- každý rámec má zcela jiný RC4 seed
- číslování rámců
- hlavní klíč PTK se pravidelně mění
- vylepšený kontrolní kód rámce



WPA - získání PTK

- vyžaduje software v klientovi, tzv. supplicant (prosebník)
- preferovaný způsob – 802.1X (dále)
- zjednodušený – předsdílený 256-bitový klíč
  - zadatelný jako heslo 8 - 63 znaků
  - 4-way handshake, umožňující hádat heslo
  - znalec hesla může zjistit PTK ostatních klientů, tzv. *nosey employee*

Wi-Fi Protected Setup

- Lidé nejsou ochotni používat pro WPA-PSK dostatečně silné heslo.
- Snaha zavést jednoduché a bezpečné nastavení, známé např. z DECT, Bluetooth
  - zadáním PIN – 8 číslic
  - stisknutím tlačítka na obou zařízeních
  - jinými metodami (NFC, Flash disk)
- Na nových zařízeních standardně zapnuto.

Zranitelnost WPS

- publikováno v prosinci 2011
  `http://code.google.com/p/reaver-wps/`
- ověření WPS PIN probíhá po polovinách
- osmá číslice je kontrolní

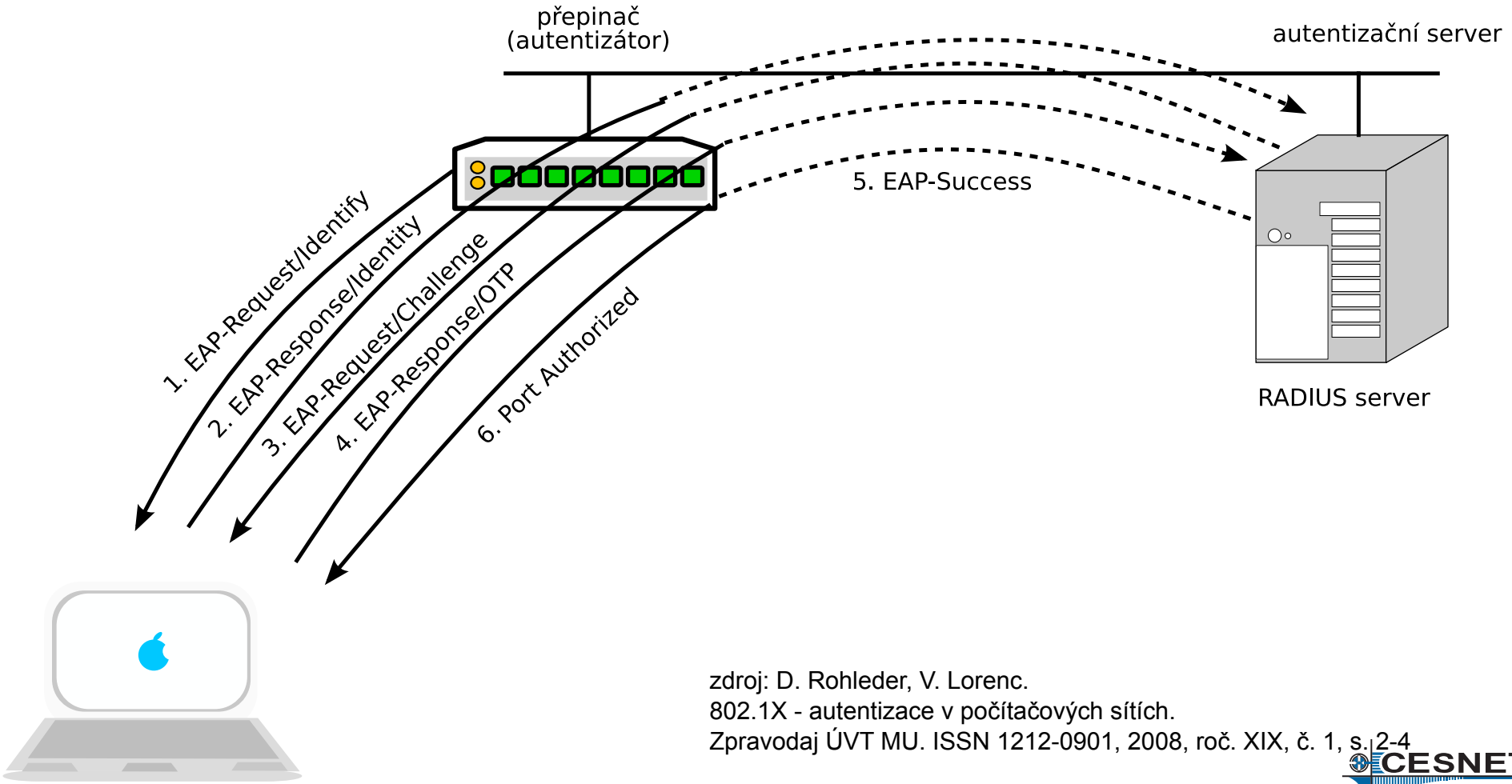
$$(10^4 + 10^3) << 10^7$$

- většina AP nemá omezení počtu pokusů
- rychlost hádání 2 - 30 sekund/pokus

IEEE 802.1X

- řízení přístupu k drátovým a bezdrátovým sítím
- provádí přímo přístupový bod – AP, switch
- využívá protokol EAP a RADIUS servery
- autentizace pomocí různých EAP metod
  - EAP-TLS – autentizace certifikátem
  - PEAP-MSCHAPv2 – nejčastější –
    – autentizace jménem a heslem, tunelováno v TLS
  - LEAP – Cisco proprietary, prolomeno – `asleap`

IEEE 802.1X - princip



zdroj: D. Rohleder, V. Lorenc.
802.1X - autentizace v počítačových sítích.
Zpravodaj ÚVT MU. ISSN 1212-0901, 2008, roč. XIX, č. 1, s. 2-4

eduroam

- Wi-Fi roaming založený na 802.1X
- projektu se účastní akademické instituce po celém světě
- člen kterékoli připojené instituce získá připojení v kterékoli instituci
- ověřování v domovské organizaci uživatele, uživatelské jméno ve tvaru `user@org.tld`

CESNET

Captive portal

- řízení přístupu úrovni IP protokolu
- bezdrátová síť otevřená, bez šifrování
- po připojení jsou všechny HTTP požadavky přesměrovány na místní bránu
- zadání přihlašovacích údajů otevře plnohodnotný přístup

Slabá místa captive portálů

- DNS tunelování (`iodine`)
  `http://code.kryo.se/iodine/`
- odposlechy
- nepohodlné
- TLS certifikáty, CRL, OCSP Pozn.: Týká se i 802.1X.
- DNSSEC?
- IP adresa 1.1.1.1 (Cisco)

Bezpečnost klientů

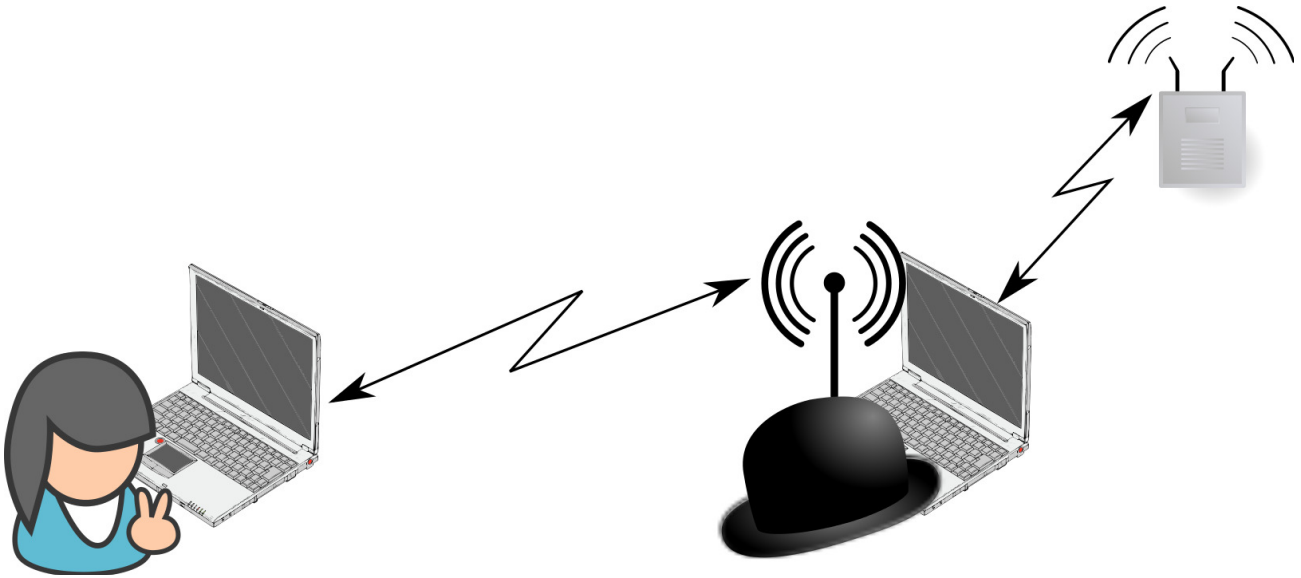
- Odposlech
- Man-in-the-middle
- Falešné sítě

Odposlech

- triviální na nešifrovaném provozu
- snadný na WEP
- proveditelný mezi uživateli WPA(2)-PSK
- proveditelný mezi uživateli WPA(2)-802.1X
  tzv. `WPA2-Hole196`

Man-in-the-middle

- útok nejen na šifrovanou komunikaci
- postup:
  1. Útočník se stane jak klientem, tak AP.
  2. Donutí klienty k reasociaci na falešné AP.
  3. Přenáší data mezi pravou a falešnou sítí.



Falešné sítě

Vylákání citlivých údajů:

1. Uživatel má v seznamu známých sítí nějakou nešifrovanou, periodicky vysílá výzvy.
2. Útočník výzvu zachytí a vyrobí pro ni AP.
3. Uživatelské zařízení se automaticky připojí do falešné sítě a začne přenášet data.
4. Útočník zjistí řadu zajímavých skutečností i z charakteru provozu.
   (Facebook, Google, Twitter, SIP)

Závěrečná doporučení

- Nepoužívejte WEP.
- Pokud vaše zařízení umí WPA2, používejte jej.
- Vypněte WPS!

  Trváte-li na WPS, přegenerujte PIN tak, aby 1. a 5. číslice byla „9“.
- Nepoužívejte *captive portal* ani pro hosty.
  - Hosté se pohodlněji připojí do 802.1X
  - Ve velkých areálech stačí „Free WIFI“
- Prověřte, jak komunikují vaše mobilní aplikace.

  Ideálně s kontrolou odolnosti proti TLS MitM.

Konec

Děkuji za pozornost.

3. – 4. března 2012

CESNET