802.11 biztonság

Mire jó a WiFi?

- Nagy sebesség – kábelek nélkül
- Kényelmes, mobil munka
- Egyszerű megoldás, amikor rövid időre kell kapcsolat
- Hatalmas területek lefedésére alkalmas
- Megoldás lehet oda, ahol nincs lehetőség kábelezésre

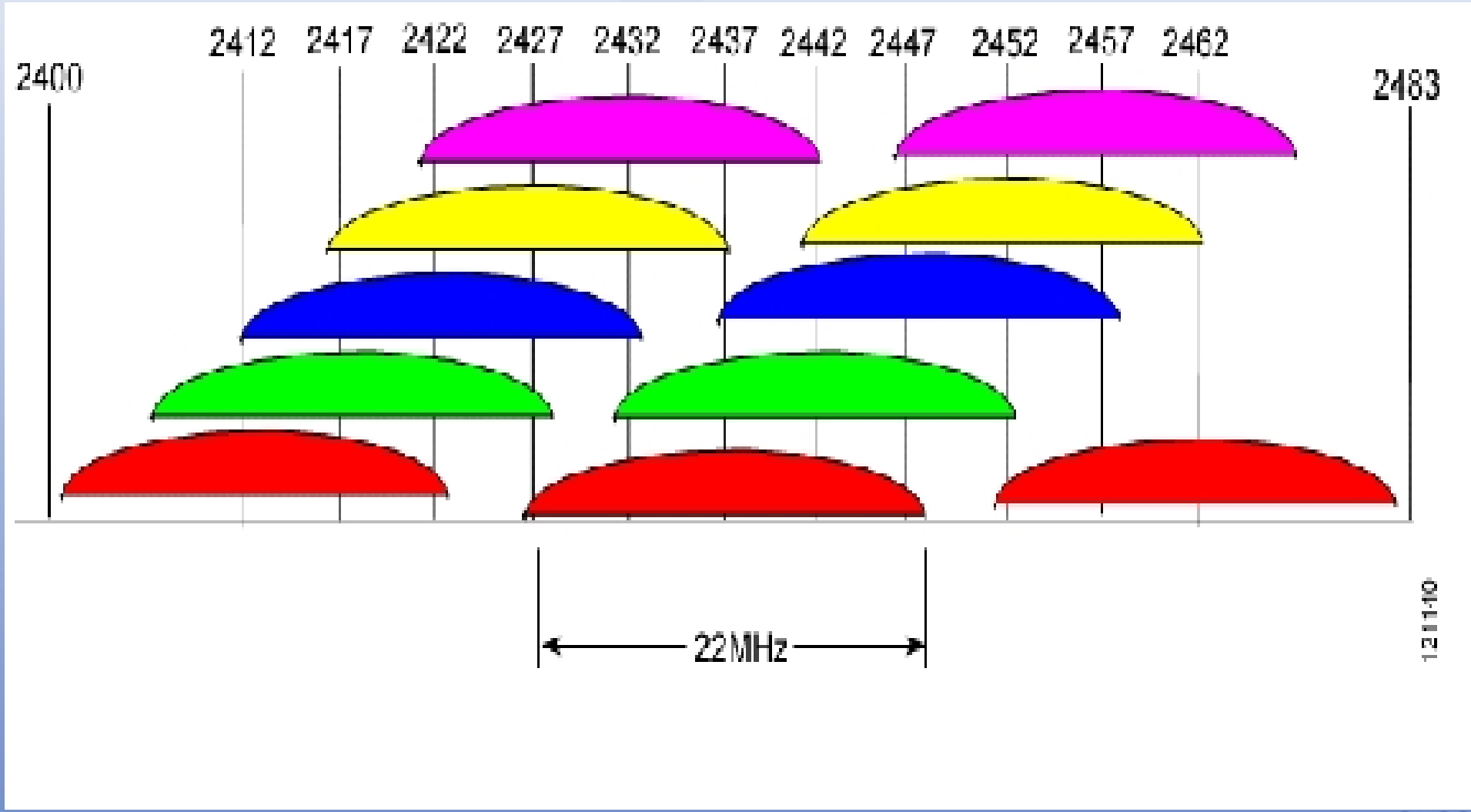
A WiFi hálózatok technikai háttere

- ISM sáv (Industrial, Scientific and Medical band)
  - rádió hullámok
  - 2,4 Ghz (802.11b, 802.11g) és 5,8 Ghz (802.11a)
- Átviteli közeg a “levegő”
- A kapcsolódás dinamikus (STA – BSS)
- A frekvenciák átfedik egymást
- A jel terjedését nem lehet behatárolni

IP TECHNOLOGIES

HUWICO

A WiFi hálózatok technikai háttere



IP TECHNOLOGIES

HUWICO

A WiFi hálózatok technikai háttere

A fizikai réteg nagyban különbözik a vezetékes hálózatoktól

- nem védett a külső jelektől
- nem megbízható a közeg
- dinamikus topológia
- a kliensek láthatatlanok lehetnek

A WiFi hálózatok technikai háttere

802.11 szolgáltatások:

Kliens (Station Services – SS)

- Authentication
- Deauthentication
- Privacy
- MSDU delivery

IP TECHNOLOGIES

HUWICO

A WiFi hálózatok technikai háttere

802.11 szolgáltatások:

Hálózat (Distribution system Services – DS)

- Association
- Diassociation
- Distribution
- Integration
- Reassociation

IP TECHNOLOGIES

HUWICO

Alapvető biztonsági kockázatok

- A technológiából adódó problémák
- “Nálam nincsen értékes adat!” - A Felhasználó
- A technológia mára jobban kiforrott, DE ...
- Konfiguráció hiánya – WZC
- Rengeteg titkosítatlan forgalom

IP TECHNOLOGIES

HUWICO

WiFi hálózatok implementálása

- Logikai tervezés
- Telepítés tervezése
- Meglevő vezeték nélküli infrastruktúra áttekintése
- Eszközök telepítése
- Biztonsági felmérés
- Karbantartási támogatás tervezése
- Gateway biztonság

IP TECHNOLOGIES

HUWICO

WiFi hálózatok implementálása

1, Logikai tervezés

- Milyen tipusú hálózat (hotspot, privát SOHO ...)
- Üzleti megfontolás
- Előzetes hálózati topológia
- Kockázatfelmérés – Risk vs. Benefit

IP TECHNOLOGIES

HUWICO

WiFi hálózatok implementálása

2, Telepítés tervezése

- Az épület tervrajzának megismerése
- Lefedettségi tervezés
- AP elhelyezés (áram, hálózat)
- Kábelezés (ha szükséges...)
- Hálózat áttekintése

IP TECHNOLOGIES

HUWICO

WiFi hálózatok implementálása

3, Meglévő infrastruktúra áttekintése

- Meglevő 802.11 eszközök (típus, szabvány ...)
- Bluetooth
- Egyéb zavaró jelek (mikrohullámú, szomszéd)

IP TECHNOLOGIES

HUWICO

WiFi hálózatok implementálása

4, Eszközök telepítése

- Eszközök beállítása, kiszerelése
- Fizikai biztonság
- Cimkézés
- Kábelezés árnyékolása
- Dokumentálás :-)

IP TECHNOLOGIES

HUWICO

WiFi hálózatok implementálása

5, Biztonsági felmérés

- Azonosítás, titkosítás
- Fölösleges funkciók kikapcsolása (UpnP, SNMP)
- Remote logolás
- Webes konfigurálás – HTTPS
- Jelerősség szabályozása

IP TECHNOLOGIES

HUWICO

WiFi hálózatok implementálása

6, Karbantartási támogatás

- Monitorozás
- Figyelmeztetési szintek meghatározása
- Incident Response – Biztonsági és technikai
- Felelősök kijelölése

IP TECHNOLOGIES

HUWICO

WiFi hálózatok implementálása

7, Gateway biztonság

- Engedett (tiltott ?) forgalom
- Hálózatok közötti átjárhatóság
- Szolgáltatások szűkítése
- Monitorozás

IP TECHNOLOGIES

HUWICO

Wardriving

- Wardrivng is still NOT a crime – elmosódó határok
- Szükséges eszközök
- Statisztika – rettenetes
    - default, linksys, SMC
    - MAC filter
    - WEP
    - WPA*

IP TECHNOLOGIES

HUWICO

A nyitott hálózatok biztonsági kockázatai

- Anonimitás
- “Az én adataim nem érdekesek senkinek”
- Visszanyomozhatatlan – kit büntessenek ?
- Botnetek
- Építsünk ISP-t!

IP TECHNOLOGIES

HUWICO

HotSpot

- Fizikai közelség
- Nincs titkosítás
  - Internet Hungary
  - CeBIT
- SSL, TLS használata kötelező!
- VPN, ha lehetséges
- MITM – Evil Twin
- A fizetős hotspotok biztonságosabbak?

IP TECHNOLOGIES

HUWICO

A biztonság illúziója

“Hall of shame”

- MAC filterezés – a tökéletes biztonság ?
- SSID broadcast tíltása
- EAP-LEAP
- DHCP tiltás
- Jelerősség és irányítás
- 802.11a

IP TECHNOLOGIES

HUWICO

VPN

- nem WiFi védelemre lett kitalálva
- layer 3 és felette
- a WiFi támadások layer 2
- szigorú tűzfalazás
- még mindíg hozzáférhető a hálózat

WEP

- WEP – Wired Equivalent Privacy
- 64 (40) és 128 (104) bit
- 1997 – 40 bit elegséges volt
  - csak lehallgatás ellen tervezték
- 802.11 – csak 40 bites definíció
- 128 (104) bit “de facto” szabvány
- 64 RC4 kulcs = 24 IV + 40 WEP kulcs
- Titkosított csomag = csomag XOR RC4 stream
- ICV – Integrity Check Value (4 byte)

WEP

Gyengeségek:

- kulcs management
- kulcs méret
- IV méret kicsi
- ICV algoritmus nem megfelelő
- RC4 implementálása gyenge
- Autentikációs üzenet hamisítás lehetséges
- CRC-32 – errorokhoz remek, hash-hez nem

IP TECHNOLOGIES

HUWICO

WEP törés

nagy számú IV kell a támadáshoz

- Lehallgatás
  - nagyon lassú (hetek)
- Authentication, Association flood
  - random MAC címekről
  - közepesen gyors
- Brute force (replay)
  - arp replay
  - valós kérés spoofolással

WPA*

802.11i – 2004

Titkosítás

WPA1 – TKIP, opcionális AES
WPA2 – AES, opcionális TKIP

Azonosítás

SOHO – PSK (Pre Shared Key)
Enterprise - EAP

IP TECHNOLOGIES

HUWICO

WPA*

WEP hibáinak javítása

- IV méret 48 bit
- CRC-32 helyett Michael (64 bit MIC)
- Master key, Temporal key
- Autómatikus kulcs-csere
- IV mint frame számláló – replay védelem

IP TECHNOLOGIES

HUWICO

WPA-PSK

PSK = Pre Shared Key

1, association
2, authentication (PMK létrehozás)
3, PTK létrehozás PMK alapján
4, sértetlenség ellenőrzése

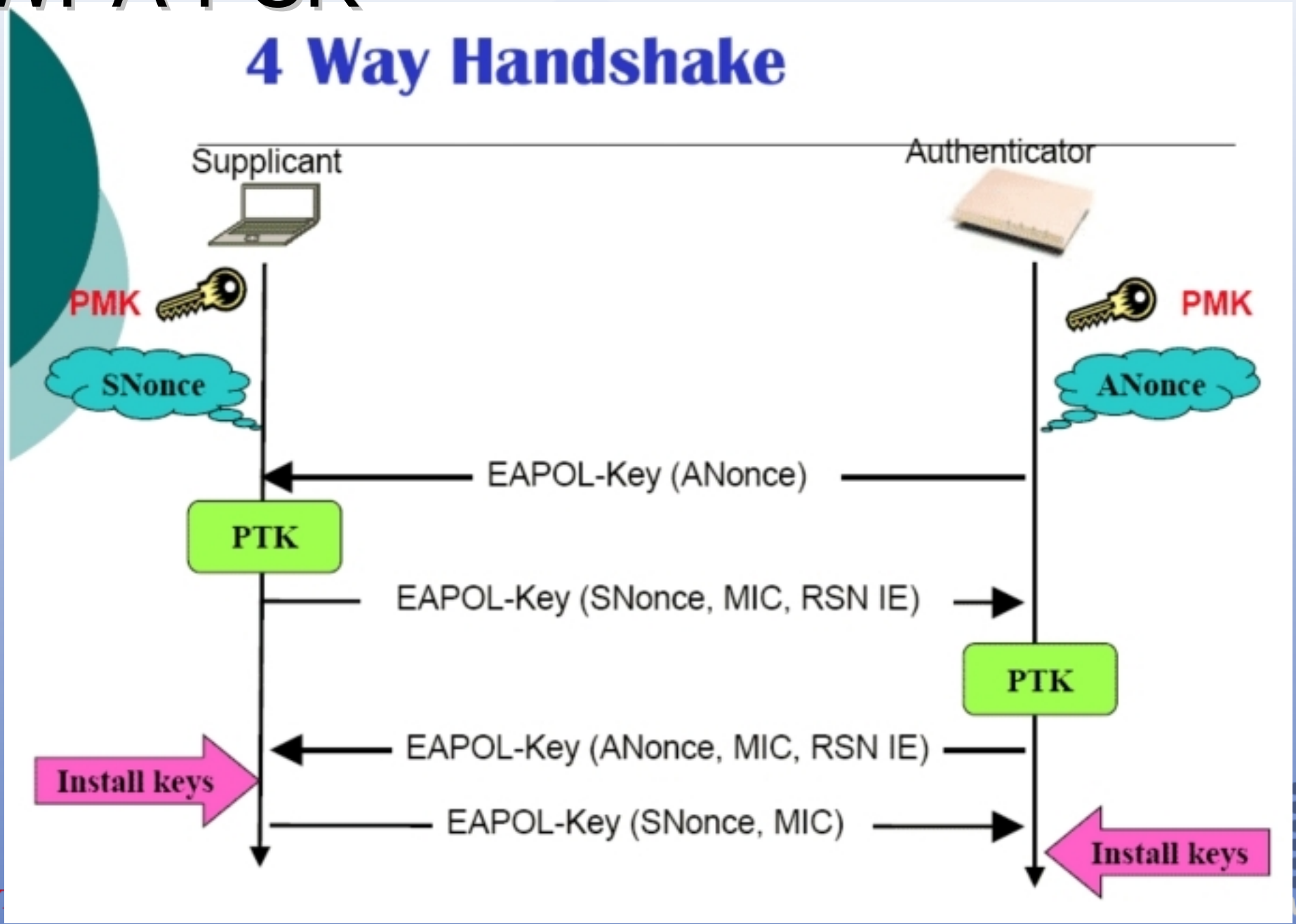
PMK = PBKDF2(pass,ssid,ssid_lenght,4096,256)
PTK = PRF512(PMK, [AP-kliens MAC], Nonce)

Törhető!

IP TECHNOLOGIES

HUWICO

WPA-PSK


4 Way Handshake
Supplicant
Authenticator
PMK
SNonce
PMK
ANonce
EAPOL-Key (ANonce)
PTK
EAPOL-Key (SNonce, MIC, RSN IE)
PTK
EAPOL-Key (ANonce, MIC, RSN IE)
Install keys
EAPOL-Key (SNonce, MIC)
Install keys

EAP

Extensible Authentication Protocol

- Framework – nem konkrét auth
- kb 40 különböző megoldás
- EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-SIM, EAP-AKA, EAP-SIM, PEAP, LEAP, EAP-TTLS
- automatikus PMK disztribúció

IP TECHNOLOGIES

HUWICO

MsCHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2

- Microsoft fejleszti
- felhasználó név clear text
- a jelszó SALT nélküli NT hash
  - lehet cleartext is
- szótáras támadással törhető
- megfelelően komplex jelszavak esetén védettebb – való életben nincsenek ilyenek

IP TECHNOLOGIES

HUWICO

EAP-LEAP

Lightweight Extensible Authentication Protocol

- Cisco implementáció
  - /felhasználó azonosítás
  - WEP gyengeségeit kívánta kiküszöbölni
- felhasználó név clear text
- jelszó MsCHAPv2
- támadható – offline brute force

EAP-MD5

- IETF nyitott szabvány
- nem WiFi hálózatokra szánták
- minimális biztonság
- felhasználó név cleartext
- jelszó MD5 hash
- offline szótáras támadás
- önmagában TILOS használni

EAP-PEAP (PEAP)

- Microsoft fejlesztés
- Első sorban Windows kliensek
- TLS session először
- nem szükséges kliens cert :-\
- gyors újrakapcsolódás
- bármilyen EAP tipus azonosításra (MsCHAPv2)

Hibás kliens konfiguráció ?

IP TECHNOLOGIES

HUWICO

EAP-TTLS

- Funk, Meetinghouse fejlesztés
- Multiplatform kliens
- TLS session először
- nem szükséges kliens cert :-\
- gyors újrakapcsolódás
- bármilyen azonosítás (radius függő)

Hibás kliens konfiguráció ?

IP TECHNOLOGIES

HUWICO

EAP-FAST

Cisco fejlesztés – LEAP helyett
0, PAC (Protected Access Credentials) distr.
1, TLS tunnel
2, Felhasználó azonosítás

PAC egyszer generálódik felhasználónként klienshez kell kerüljön – 0. fázis

Csak marketing

IP TECHNOLOGIES

HUWICO

EAP-TLS

- IETF nyitott szabvány
- Teljes körű támogatottság
- Szerver ES kliens oldali cert szükséges
- Lassú újrakapcsolódás – roaming

Jelen pillanatban Tokennel használva a legbiztonságosabb megoldás

IP TECHNOLOGIES

HUWICO

Összefoglalás

- Remek dolog a WiFi
- A technológia mára már kiforrott
- A felhasználó és a policy a gyenge pont
- Oktatás és egészséges paranoia szükséges

IP TECHNOLOGIES

HUWICO

Köszönöm a figyelmet!

Horváth Tamás
kodmon@huwico.hu

IP TECHNOLOGIES

HUWICO