

Vezetéknélküli hozzáférés

Enterprise WLAN



Hálózatok építése, konfigurálása és működtetése

Vezetéknélküli hálózatok



Wireless Fidelity (WiFi)

- ▶ **WiFi - Wireless Fidelity**
 - ▶ Maximum: kb. 200 m, 300 Mbps (1 Gbps)
 - ▶ Világrekordok (erősítés nélkül)
 - ▶ 200km - USA, Las Vegas
 - ▶ 304km – Olaszország
 - ▶ 382km (3Mbps) - Venezuela



Vezetéknélküli hálózatok – miért is?

- ▶ **Előnyök a korábbi vezetékes hálózatokkal szemben**
 - ▶ **Felhasználók**
 - ▶ Az Intranet és Internet elérése vezetékek nélkül (vezetékes telefon és vezetéknélküli telefon)
 - ▶ Csatlakozás a frekvenciált helyeken (HOTSPOT)
 - Reptéri terminálok
 - Kávézók, szórakozóhelyek
 - Szállodák
 - ▶ **Adminisztrátorok**
 - ▶ Könnyen üzembe helyezhető
 - ▶ Olyan helyekre is elvihető, ahova vezetékeket nehezen lehet kihúzni
 - ▶ **Üzleti szempont**
 - ▶ Hosszútávon olcsóbb üzemeltetni, beruházás is olcsóbb lehet
 - ▶ HotSpot esetében a felhasználók fizetnek a szolgáltatásért
 - ▶ **WiFi offload – Tehermentesíteni más (mobil) hálózatokat**

Vezetéknélküli hálózat elemei

▶ Vezetéknélküli hálózati kártya

- ▶ Leginkább könnyen mozgatható eszközökhöz Laptop, PDA és TablePC
 - ▶ De ma már fényképezőgép, videójáték, mobiltelefon ...
- ▶ Beépített eszközök, PCMCIA, CF kártya, USB eszköz, stb..
- ▶ Egyedi MAC cím

▶ Hozzáférési pont (Access Point – AP)

- ▶ A vezetéknélküli eszközök rádiókapcsolatban vannak a hozzáférési ponttal



IEEE 802.11 család

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11f - Inter-Access Point Protocol (2003)
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)
- IEEE 802.11k - Radio resource measurement enhancements
- IEEE 802.11l - (reserved, typologically unsound)
- IEEE 802.11m - Maintenance of the standard; odds and ends.
- IEEE 802.11n - Higher throughput improvements
- IEEE 802.11o - (reserved, typologically unsound)
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
- IEEE 802.11q - (reserved, typologically unsound, can be confused with 802.1q VLAN trunking)
- IEEE 802.11r - Fast roaming
- IEEE 802.11s - ESS Mesh Networking
- IEEE 802.11t - Wireless Performance Prediction (WPP) - test methods and metrics
- IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless network management
- IEEE 802.11w - Protected Management Frames
- IEEE 802.11y - 3650-3700 MHz Operation in USA
- IEEE 802.11z - Extensions to Direct Link Setup
- IEEE 802.11aa - Video Transport Streams (2012)
- IEEE 802.11ac - Very High Throughput 6GHz (2013)
- IEEE 802.11ad - Very High Throughput 60GHz (2012)
- IEEE 802.11ae - Prioritization of Management Frames (2012)
- IEEE 802.11af - TV White Spaces (2014)
- IEEE 802.11ah - Sub 1 GHz
- IEEE 802.11ai - Fast Initial Link Setup
- IEEE 802.11aj - China Millimeter Wave
- IEEE 802.11ak - General Link
- IEEE 802.11aq - Pre-Association Discovery
- IEEE 802.11ax - Next Generation
- IEEE 802.11ay - Next Generation 60GHz



WiFi Biztonság

Vezetéknélküli hálózatok kihívásai

▶ Legfőbb kihívások

- ▶ Rádióhullámok (csatornák) interferenciája
 - ▶ Több hozzáférési pont elhelyezése
 - ▶ Egymást zavaró adások/zajok
 - ▶ Tereptárgyak hatásai
- ▶ Eszközök tápellátása (részben vezetékes..)
 - ▶ Tápfelhasználás optimalizálása
- ▶ Mozgás a hozzáférési pontok között
 - ▶ AP váltás, szolgáltató-váltás, technológia váltás
- ▶ **Biztonság**

Vezetéknélküli hálózatok biztonsága

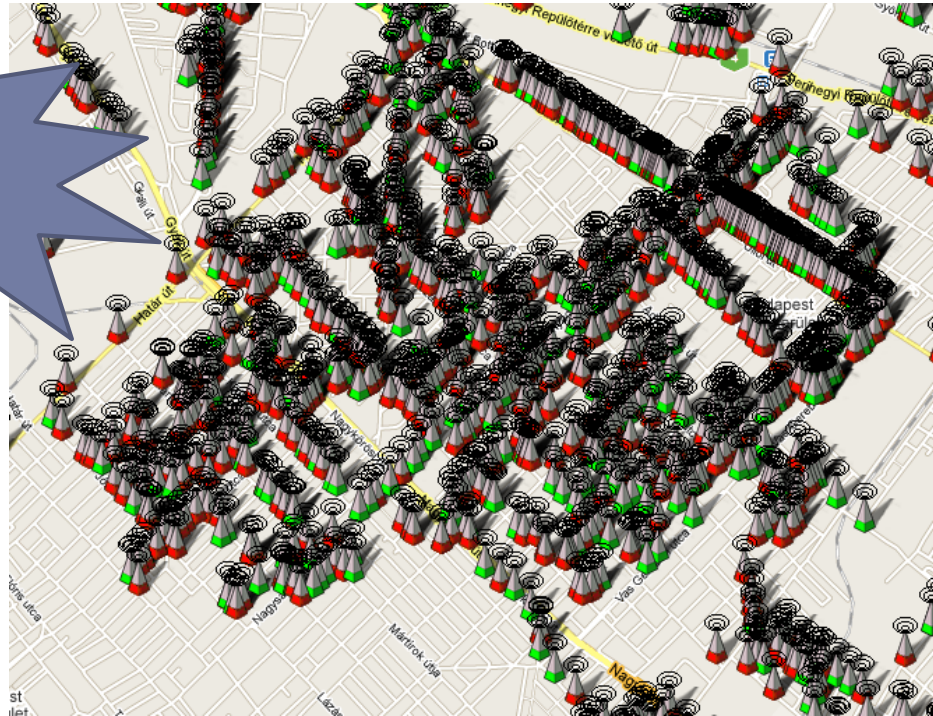
- ▶ Vezetékes hálózat esetében az infrastruktúrához való hozzáférés már sok behatolót megállít
- ▶ Vezetéknélküli hálózat esetén azonban megszűnik ez a korlát
 - ▶ A fizikai közeg nem biztosít adatbiztonságot, a küldött/fogadott adatokat mindenki észleli
 - ▶ A támadó nehézségek nélkül és észrevétlenül hozzáfér a hálózathoz
 - ▶ Sokszor a hálózat eljut az lefedni kívánt területen kívülre is

Vezetéknélküli hálózatok biztonsága 2.

- ▶ **Felmerülő biztonsági kérdések**
 - ▶ Hálózat elérésének korlátozása
 - ▶ Hitelesítés
 - ▶ A felhasználó hitelesítése
 - ▶ A szolgáltató hitelesítése
 - ▶ Sikeres hitelesítés után az adatok védelme
 - ▶ Infrastruktúra védelme
 - ▶ Anonimitás (jelenleg nem cél)

Wardriving

Évekkel
ezelőtt



www.wifiterkep.hu:

AP titkosított:	61%
(16247db)	
AP nyílt:	39%
(10451db)	

Hitelesítés problémái

- ▶ **Kihívás-válasz alapú hitelesítés**
 - ▶ Vezetékes környezetben jól működik
 - ▶ A felhasználó általában bízhat a vezeték épségében
 - ▶ Vezetéknélküli környezetben már nem tökéletes
 - ▶ A támadó könnyen megszerezheti a kihívást és a választ is
 - ▶ Gyenge jelszavak (és protokollok) eseték egyszerű a szótáras támadás

Szolgáltatásbiztonság problémái

- ▶ **Hamis hozzáférési pontok (rogue AP)**
 - ▶ Könnyű elrejtteni – egy SD kártya is lehet AP!
 - ▶ Lehet falakon kívül is (irányított antennák)
 - ▶ A felhasználó nem feltétlenül ismeri
Pl.: HOTSPOT környezet
 - ▶ Segítségével közbeékelődéses (man-in-the-middle) támadások
- ▶ **Szolgáltatásmegtagadás DoS**
 - ▶ Szolgáltatásmegtagadás elárasztással egy vezetékes eszköztől
 - ▶ Fizikai akadályoztatás (jammer)



Hozzáférés vezérlés – MAC szűrés

- ▶ Hozzáférés szűrése MAC címek alapján
 - ▶ A hozzáférési pontnak listája van az engedélyezett kártyákról (vagy tiltott kártyák)
 - ▶ Nem biztonságos, mert:
 - ▶ A MAC címek lehallgathatóak a hálózaton és felvehetőek egy másik eszköz által
 - ▶ Az eszközök megszerzése már hozzáférést biztosít
 - ▶ Több hozzáférési pont menedzsmentje nehéz
- ▶ Sajnos ma is ez van a sok „biztonságos” helyen



BME

Hozzáférés vezérlés – SSID tiltás

- ▶ A hozzáférési pontok elrejtése
 - ▶ A hozzáférési pont nem közli a saját azonosítóját (Service Set ID - SSID)
 - ▶ Csak azok a készülékek csatlakozhatnak, akik ismerik ezt
 - ▶ PROBE request
 - ▶ Lehallgatással felderíthető!

www.wifiterkep.hu:

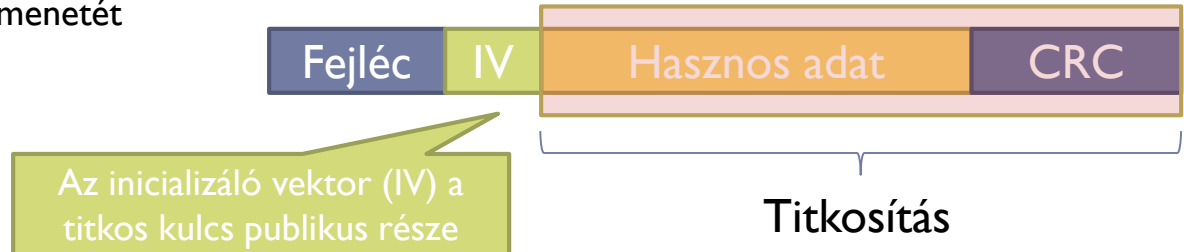
TOP 10 ESSID (hálózatnév):	
ESSID:	darabszám:
SMC	1274
linksys	1013
default	1003
TP-LINK	500
NETGEAR	437
dlink	409
belkin54g	322
GIGABYTE	213
WIERA	195
WLAN	150

Hozzáférés vezérlés - WEP

- ▶ Hitelesítés és adatkommunikáció védelem a WEP protokollal
 - ▶ Wired Equivalent Privacy
 - ▶ Kitűzött cél: Pont olyan védett, mintha vezetékes lenne
- ▶ Hitelesítés és titkosítás
 - ▶ Hitelesítés: az eszköz ismeri a WEP kulcsot
 - ▶ Nem a felhasználót hitelesítjük, hanem az eszközt
 - ▶ RC4 titkosító használata (gyors!)
 - ▶ CRC32 hibajelző kód (gyakran használjuk)
 - ▶ Cyclic Redundancy Check
 - ▶ Titkosítjuk a hibajelző kimenetét



- ▶ Kihívás – válasz alapú hozzáférés vezérlés



WEP törések

▶ 2002

- ▶ „Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, A. Stubblefield, J. Ioannidis, A. Rubin”
 - ▶ Gyenge WEP IV-k
 - ▶ 4.000.000 – 6.000.000 csomag

▶ 2004

- ▶ KoReK, fejlesztett FMS támadás
 - ▶ 500.000 – 2.000.000 csomag (104 bites WEP)

▶ 2006

- ▶ KoReK, Chopchop támadás
 - ▶ Az AP segítségével a titkosított CRC miatt bájtonként megfejthető a titkosított üzenet

▶ 2007

- ▶ PTW (Erik Tews, Andrei Pychkine and Ralf-Philipp Weinmann), még több korreláció
 - ▶ 60.000 – 90.000 csomag (104 bites WEP)

WEP hibák

▶ HIBA 1:

- ▶ Az titkos kulcs és a publikus IV egyszerűen csak illesztve van. Ennek segítségével az RC4 kimenetéből kiszámítható a titkos kulcs!!!

▶ HIBA 2:

- ▶ A titkos kulcs kezdetben túlságosan rövid, mindössze 40 bit. Ma 104 bit.

▶ HIBA 3:

- ▶ Az IV túlságosan rövid (24 bit) és nincsen egyértelmű utasítás hogyan alkalmazzuk. A megismételt sorszám felfedheti a titkosított adatot. Sok eszköz mindig nullázta az IV-t induláskor. Szülinapi paradoxon miatt, amúgy is ütközés 2^{12} véletlen sorszám után

▶ HIBA 4:

- ▶ A titkosított CRC32 kód nem véd. Az értéke kiszámítható a változás ismeretében

▶ **Hamis biztonságérzet!**

Adatszerzés WEP töréshez

- ▶ **Hamisított csomagok**
 - ▶ De-authentication
 - ▶ ARP response kicsikarása
 - ▶ Módosított ARP request / Gratuitous ARP üzenet
 - ▶ WEP esetén könnyen módosítható a titkosított ARP is (rossz integritás védelem)
- ▶ **„Caffé latte” támadás**
 - ▶ Nem szükséges a WEP hálózatban lenni
 - ▶ A PC/smartphone tárolja a WEP kulcsokat, a hamis AP megtévesztheti
 - ▶ Hamis ARP üzenetekkel 90.000 csomag gyűjtése
 - ▶ 6 perces támadás



WEP patch

- ▶ Nagy kulcsok
- ▶ Gyenge IVk elkerülése
- ▶ ARP filter
- ▶ WEP Chaffing
 - ▶ Megtévesztő WEP csomagok injektálása. Hatására a WEP törésnél hibás adatok alapján számolódik a kulcs
 - ▶ A törő algoritmusok javíthatóak..

802.1X - IEEE Standard for port-based Network Access Control (PNAC)

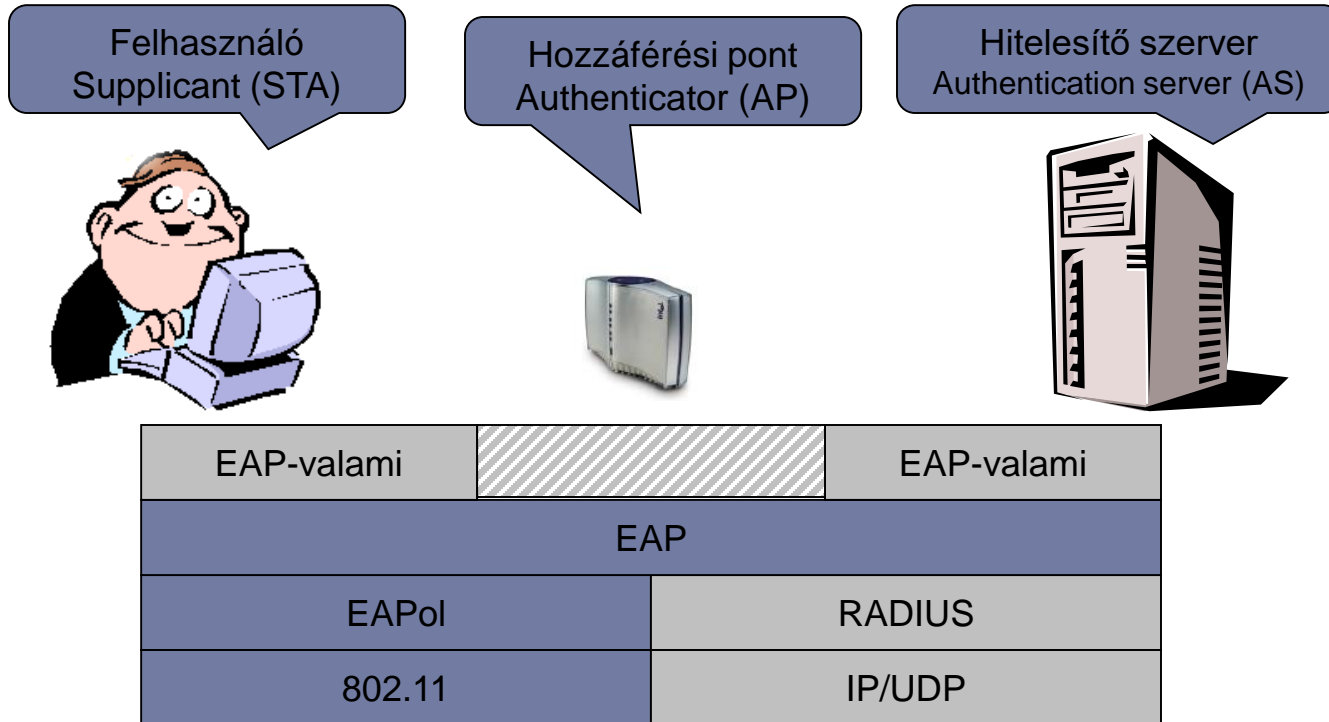
802.1x

- ▶ IEEE specifikáció a (W)LAN biztonság javítására (2001)
 - ▶ Protokollok a hitelesítés és az adatok védelmére
 - ▶ RADIUS (de facto)
 - Hitelesítés a hozzáférési pontokon túl
 - Széles körben elfogadott és alkalmazott hitelesítési módszer
 - ▶ EAP és EAPoL (EAP over Lan)
 - Transzport protokoll a biztonság (hitelesítés és adatvédelem) egyeztetésére
 - EAP-MD5 Challenge, EAP-TLS, LEAP (EAP-Cisco Wireless), PEAP
 - ▶ Nagyon jól illik WLAN környezetbe:
 - Felhasználó alapú hitelesítés
 - A hozzáférési pont nem ismeri a hitelesítést (egyszerű és olcsó)
 - Központosított hitelesítés

802.1x és WEP

- ▶ **Nem célja, hogy javítsa a WEP hibáit!**
 - ▶ Az adatok biztonságát továbbra is a WEP biztosítja (így persze nem ér semmit)
 - ▶ De a 802.1x képes kulcsot egyeztetni az adattitkosítás számára is
- ▶ **Új protokollok a WEP javítására**
 - ▶ TKIP, CCMP, WRAP
 - ▶ Együttműködnek a 802.1x protokollal

802.1x protokollok

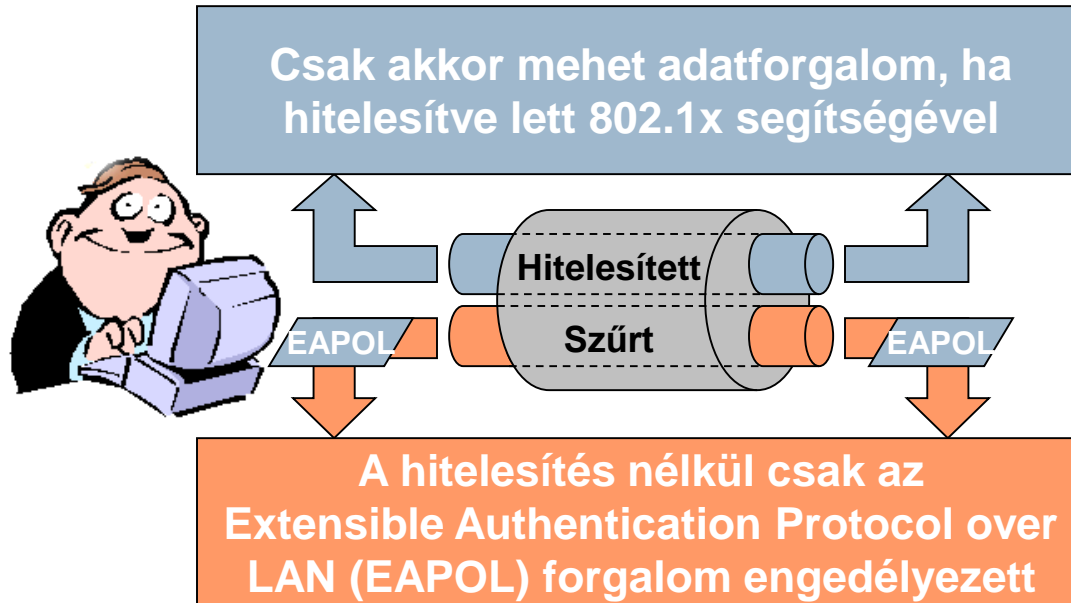


EAPoL (EAPoW)

- ▶ EAP over LAN: EAP adaptáció a port alapú (802.1X) környezethez
- ▶ EAPoL kerettípusok:
 - ▶ EAP keret
 - ▶ Beágyazott EAP keret
 - ▶ EAPoL-Start
 - ▶ A kliens küldi, hogy elindítsa az EAP kommunikációt. Hatására EAP-Request/Identity jön
 - ▶ EAPoL-Logoff
 - ▶ Port lezárása
 - ▶ EAPoL-Key
 - ▶ Kulcscsere
 - ▶ EAPoL-Encapsulated-ASF-Alert
 - ▶ Riasztások engedélyezése az adott porton. (Pl. SNMP trap)

Hozzáférés szűrés

- ▶ Kezdetben csak EAPoL forgalom



Kulcsok

▶ Master Key (MK)

- ▶ A viszony alatt fennálló szimmetrikus kulcs a felhasználó (STA) és a hitelesítő szerver között (AS)
- ▶ Csak ők birtokolhatják (STA és AS)
- ▶ Minden más kulcs ebből származik

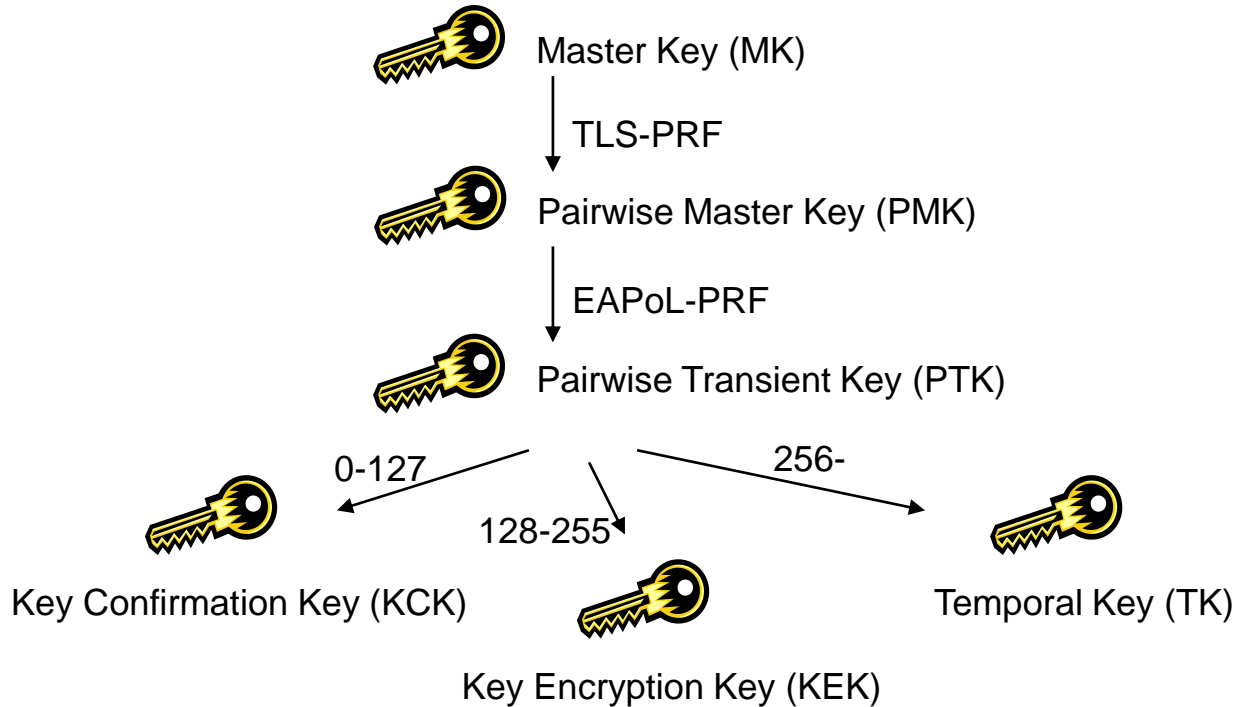
▶ Pairwise Master Key (PMK)

- ▶ Frissített szimmetrikus kulcs a felhasználó (STA) és a hozzáférési pont (AP) között
- ▶ A felhasználó (STA) generálja a kulcsot MK alapján
- ▶ A hozzáférési pont (AP) a hitelesítő szervertől (AS) kapja

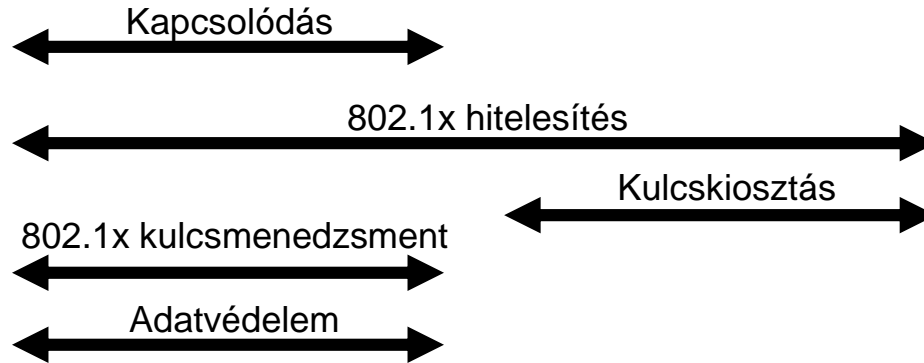
Kulcsok (folyt.)

- ▶ **Pairwise Transient Key (PTK)**
 - ▶ A felhasznált kulcsok gyűjteménye
 - ▶ Key Confirmation Key (PTK bitek 1-128)
 - ▶ A PMK ismeretének bizonyítása
 - ▶ Key Encryption Key (PTK bitek 129-256)
 - ▶ Más kulcsok terjesztése
 - ▶ Temporal Key (TK) (PTK bitek 257-..)
 - ▶ Az adatforgalom biztosítása

Kulcs hierarchia



802.1x működési fázisok



802.1x működési fázisok (folyt.)

▶ Kapcsolódás

- ▶ A kommunikáló felek megállapítása (STA és AP)
- ▶ A hozzáférési pont (AP) képességeinek ismertetése

▶ 802.1x hitelesítés

- ▶ Központosított döntés a hitelesítő szervernél (AS)
- ▶ A felhasználó (STA) eldönti, hogy kíván-e csatlakozni
- ▶ A felek (STA és AS) kölcsönös azonosítása
- ▶ Master kulcs (MK) és Pairwise Master kulcs (PMK) generálása

802.1x működési fázisok (folyt.)

▶ Kulcskiosztás

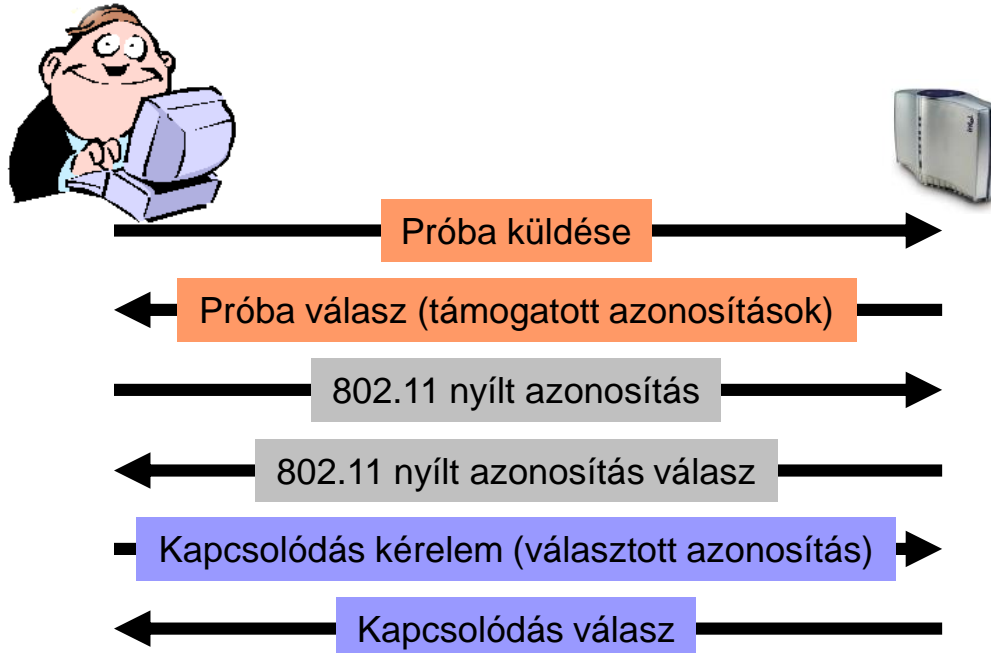
- ▶ A Pairwise Master kulcs (PMK) mozgatása a hozzáférési ponthoz (AP)

▶ 802.1x kulcsmenedzsment

- ▶ A PMK hozzárendelése a felekhez (STA és AP) + ellenőrzés
- ▶ Friss kulcsok generálása (PTK) és szétosztása

Kapcsolódás

- ▶ Kapcsolódás (authentication + association)



Kapcsolódás lépései

I. Beacon vagy Probe (próba) küldése és válasz

- ▶ Az AP tulajdonságai:
 - ▶ SSID:Az hozzáférési pont azonosítása
 - ▶ Támogatott hitelesítések
 - ▶ Támogatott unicast/multicast titkosítások
- ▶ Biztonság szempontból nem számít, bár néha elhagyják az SSID-t
 - ▶ „nem látható hálózatok”

Képesség felderítés lépései (folyt.)

2. 802.11 nyílt azonosítás

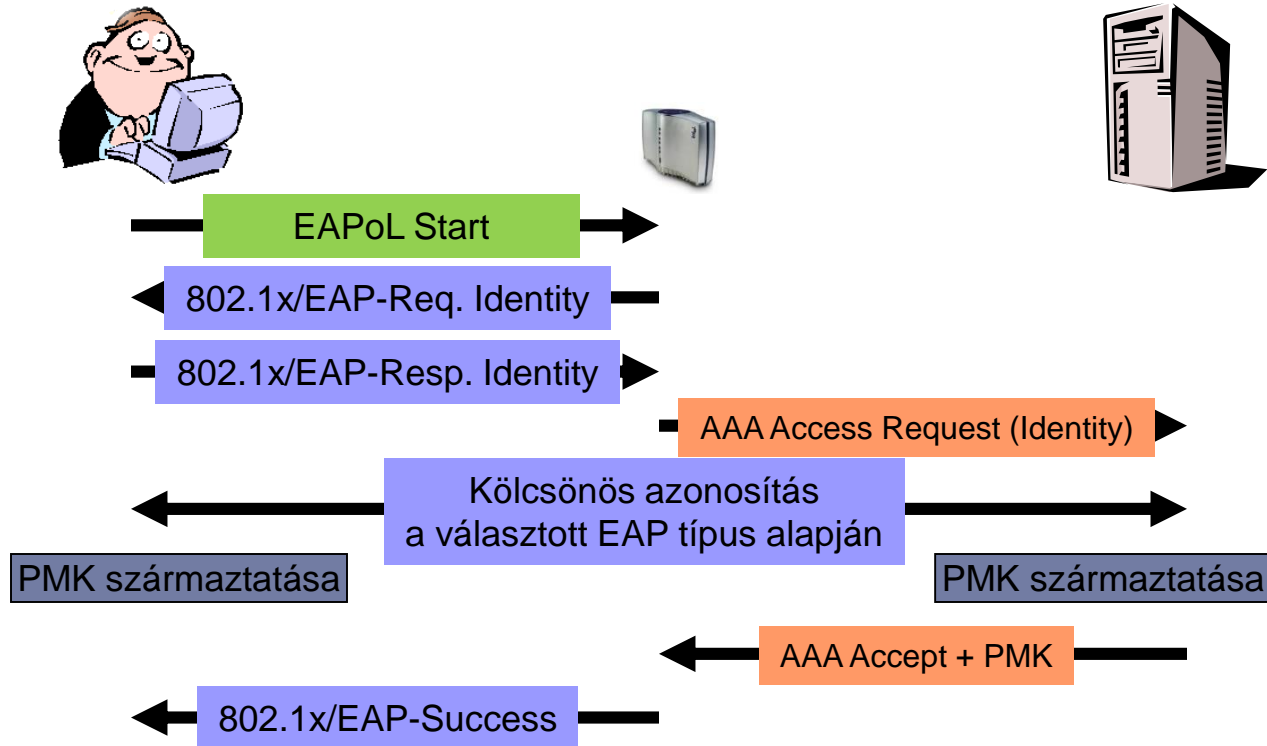
- ▶ Kompatibilitás miatt tartották meg
- ▶ Semmi biztonság nincs benne
- ▶ Létezik közös titok alapú hitelesítés is, ez a WEP alapján működik (hamisítható)

3. Kapcsolódás (asszociáció) kérelem/válasz

- ▶ A hozzáférési pont által hirdetett hitelesítés kiválasztása

- ▶ Itt még nincs biztonság semmilyen szinten!
- ▶ A felek készek a hitelesítésre és a kommunikációra

802.1x hitelesítés



802.1x hitelesítés lépései

- ▶ A hitelesítést a felhasználó indítja, de a hitelesítő szerver (AS) választja meg a módszert
 - ▶ A hitelesítő legtöbbször RADIUS szerver
 - ▶ Tapasztalatok, fejlesztések
 - ▶ A hitelesítő módszer legtöbbször EAP-TLS, EAP-TTLS vagy PEAP
 - ▶ Több kell, mint kihívás alapú hitelesítés
 - ▶ Privát/publikus kulcsok használata
- ▶ Sikeres hitelesítés esetén a hozzáférési pont (AP) megkapja a Pairwise Master Key (PMK) –t is
- ▶ Otthoni és ad-hoc környezetben nem szükséges hitelesítő központ
 - ▶ Pre-shared Key (PSK) használta PMK helyett
 - ▶ Az otthoni felhasználó ritkán kezel kulcsokat..

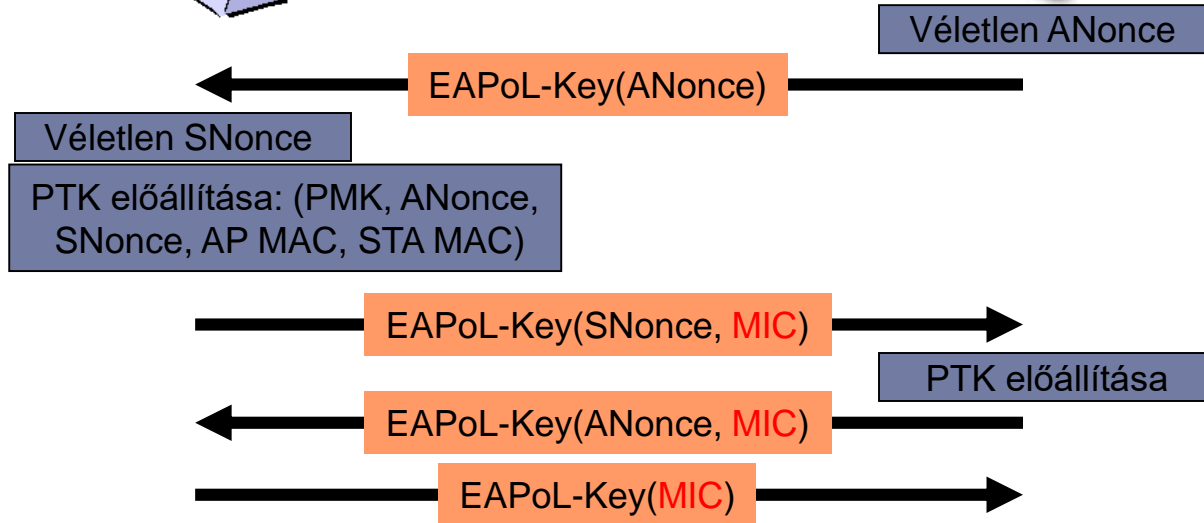
802.1x hitelesítés gondok

- ▶ **Az EAP nem biztosít védelmet**
 - ▶ Hamisított AAA-Accept üzenetek
- ▶ **RADIUS**
 - ▶ Statikus kulcs a hozzáférési pont (AP) és a hitelesítő szerver (AS) között
 - ▶ A hozzáférési pont minden üzenettel együtt egy kihívást is küld
 - ▶ Hamisított üzenetekre a RADIUS szerver gond nélkül válaszol
 - ▶ Megoldást a DIAMETER hitelesítő jelenthet
 - ▶ Sajnos úgy látszik ez sem fogja tökéletesen megoldani a problémát

802.1x kulcsmenedzsment

- ▶ A Pairwise Master Key (PMK) segítségével a felhasználó (STA) és a hozzáférési pont (AP) képes előállítani a Pairwise Transient Key (PTK) –t
 - ▶ A PMK kulcsot (ha a hitelesítő szerverben (AS) lehet bízni, akkor csak ők ismerik)
 - ▶ A PTK kulcsot mindketten (STA és AP) származtatják (nem utazik a hálózaton!) és ellenőrzik, hogy a másik fél valóban ismeri
 - ▶ 4 utas kézfogás
 - ▶ A többi kulcsot vagy egyenesen a PTK –ból származtatják (megfelelő bitek) vagy a KEK segítségével szállítják a hálózaton (pl. Group TK)

4 utas kézfogás



4 utas kézfogás lépései

- ▶ MIC: Az üzenetek integritásának védelme
- ▶ Man-in-the-middle támadások kizárása
 - ▶ A 2. üzenet mutatja, hogy
 - ▶ A felhasználó (STA) ismeri PMK –t
 - ▶ A megfelelő ANonce –t kapta meg
 - ▶ A 3. üzenet mutatja, hogy
 - ▶ A hozzáférési pont (AP) ismeri PMK –t
 - ▶ A megfelelő SNonce –t kapta meg
- ▶ A 4. üzenet csak azért van, hogy teljes legyen a kérdés/válasz működés

Krackattacks

- ▶ Discovered in 2017, fix ?
- ▶ Key Reinstallation Attacks
 - ▶ A 4 utas kézfogás meghackelése, régi kulcs visszaállítása
 - ▶ Minden számláló visszaáll az eredeti értékre és az „új” régi kulcsot használják
- ▶ Az üzenetek elveszhetnek természetes módon is
 - ▶ Ha a 3. üzenet elvész, az AP új üzenetet küld
 - ▶ Ha a kliens megkapja a 3. üzenetet, akkor onnan újraindul a protokoll
- ▶ Teljesen nulla titkosító kulcs???
 - ▶ Linux & Android wpa_supplicant
 - ▶ „Töröld a kulcsot használat után!” (mert ez így biztonságos) ...

Adatvédelem

- ▶ A TK (multicast esetén Group Transient Key - GTK) felhasználható az adatok titkosítására
 - ▶ A kulcsot a hitelesítés mellett egyeztetik (melléktermék)
- ▶ Felhasználható titkosítások:
 - ▶ TKIP
 - ▶ CCMP
 - ▶ WRAP (Patent gondok, nincs a szabványban)

WPA – WiFi Protected Access

WPA - Wi-Fi Protected Access

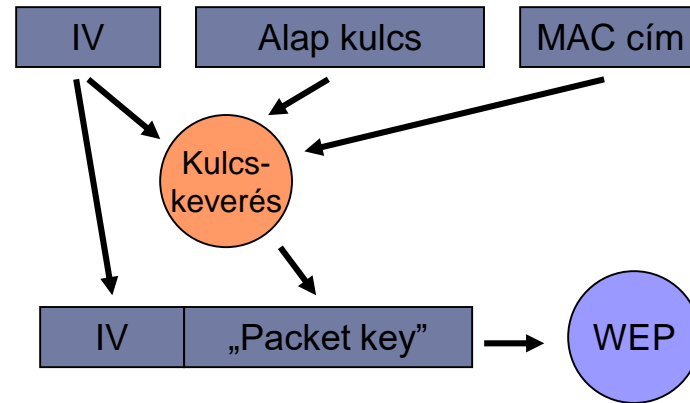
- ▶ Wi-Fi Alliance a WEP problémáinak kijavítására (2003)
 - ▶ Szabványokon alapuló
 - ▶ Erős biztonság
 - ▶ Hitelesítés és adatbiztonság
 - ▶ **Minden környezetben (SOHO és Enterprise)**
 - ▶ A meglévő eszközökön csak SW frissítés
 - ▶ Kompatibilis a közelgő 802.11i szabvánnyal
- ▶ A fokozott biztonság mellett cél a gyors elterjedés is!

WPA - TKIP

- ▶ A WEP összes ismert hibájának orvoslása, megőrizve minél több WEP blokkot
- ▶ **Titkosítás: Temporal Key Integrity Protocol (TKIP)**
 - ▶ Per-packet key mixing (nem csak hozzáfűzés)
 - ▶ Message Integrity Check (MIC) - Michael
 - ▶ Bővített inicializáló vektor (48 bit IV) sorszámozási szabályokkal
 - ▶ Idővel lecserélt kulcsok (Nem jó, de muszáj)
- ▶ **Hitelesítés: 802.1x és EAP**
 - ▶ A hitelesítés biztosítása
 - ▶ Kölcsönös hitelesítés is (EAP-TLS)
 - ▶ A hitelesítés változhat a környezettől függően (SOHO <> Enterprise <> HOTSPOT)

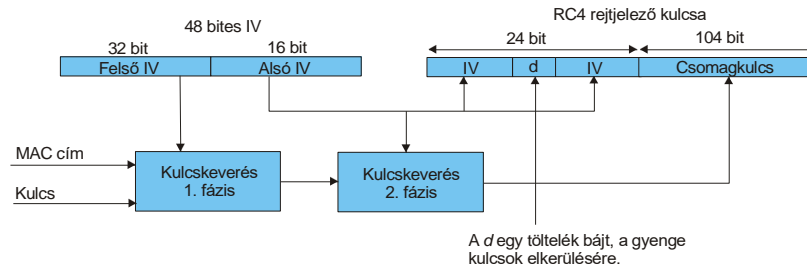
TKIP

- ▶ Per Packet Keying
- ▶ Az IV változásával minden üzenetnek más kulcsa lesz
- ▶ Minden terminálnak más kulcsa lesz, akkor is, ha az alap kulcs véletlenül egyezne
- ▶ A packet kulcsot használjuk az eredeti WEP kulcs helyett



TKIP – kulcs keverés

- ▶ 128 bites ideiglenes kulcs
- ▶ Csomagkulcs előállítása 2 lépésben
 - ▶ Feistel alapú kódoló használata (Doug Whiting és Ron Rivest)
 - ▶ 1. lépés
 - ▶ A forrás MAC címének, az ideiglenes kulcsnak és az IV felső 32 bitjének keverése
 - ▶ Az eredmény ideiglenesen tárolható, 2^{16} kulcsot lehet még előállítani. Ez javítja a teljesítményt
 - ▶ 2. lépés
 - ▶ Az IV és a kulcs függetlenítése



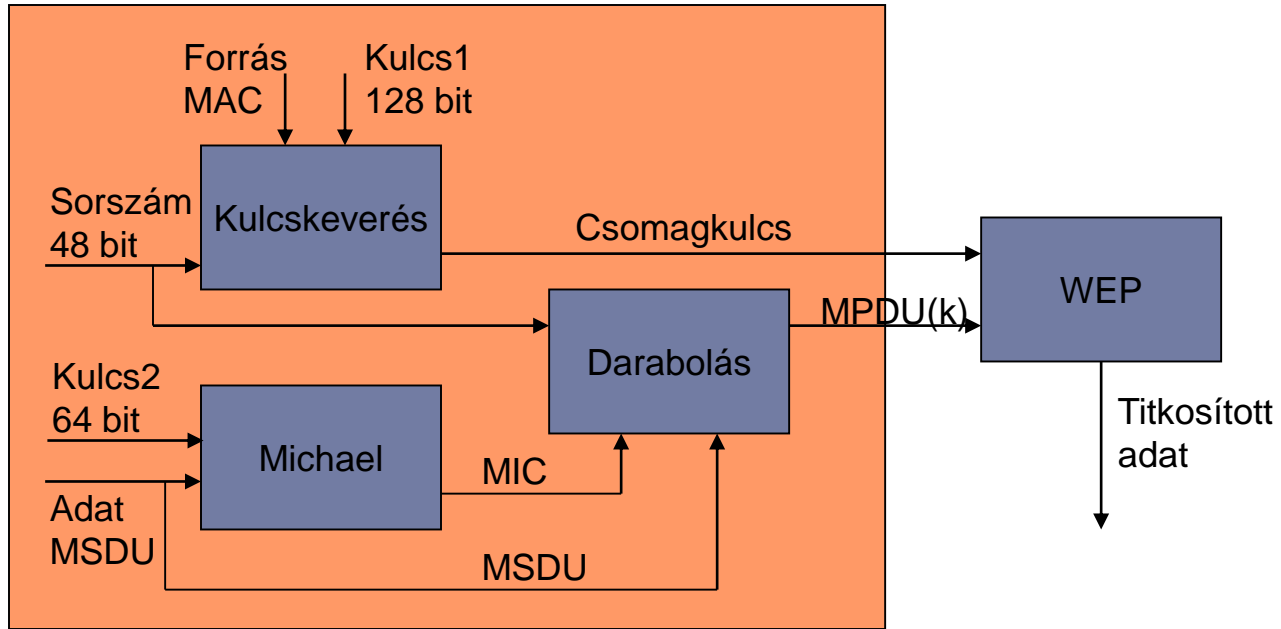
IV sorszámozás

- ▶ **IV szabályok**
 - ▶ Mindig 0-ról indul kulcskiosztás után
 - ▶ Ellentétben a WEP-pel, itt ez nem gond, mert úgy is más kulcsunk lesz minden egyeztetésnél
 - ▶ Minden csomagnál eggyel nő az IV
 - ▶ Ha nem, akkor eldobjuk az üzenetet
- ▶ **A 48 bites IV már nem merül ki**
 - ▶ Ha mégis, akkor leáll a forgalom

MIC

- ▶ Message Integrity Code
- ▶ Michael algoritmus (Neils Ferguson)
 - ▶ 64 bites kulcs 64 bites hitelesítés
 - ▶ Erőssége: kb. 30 bit, azaz a támadó 2^{31} üzenet megfigyelésével képes egy hamisat létrehozni
 - ▶ Nem túl erős védelem
 - ▶ De egy erősebb (HMAC-SHA-1 vagy DEC-CBC-MAC) már nagyon rontaná a teljesítményt
 - ▶ + védelem: ha aktív támadást észlel, akkor azonnal megváltoztatja a kulcsot + 1 percig nem enged újra változtani
 - ▶ Már nem csak az adatot védjük, hanem a forrás és cél MAC címeket is!
 - ▶ Nincs külön sorszámozás, a visszajátszás elleni védelem úgy van biztosítva, hogy a MIC értéket titkosítjuk (itt van sorszám)

TKIP működése

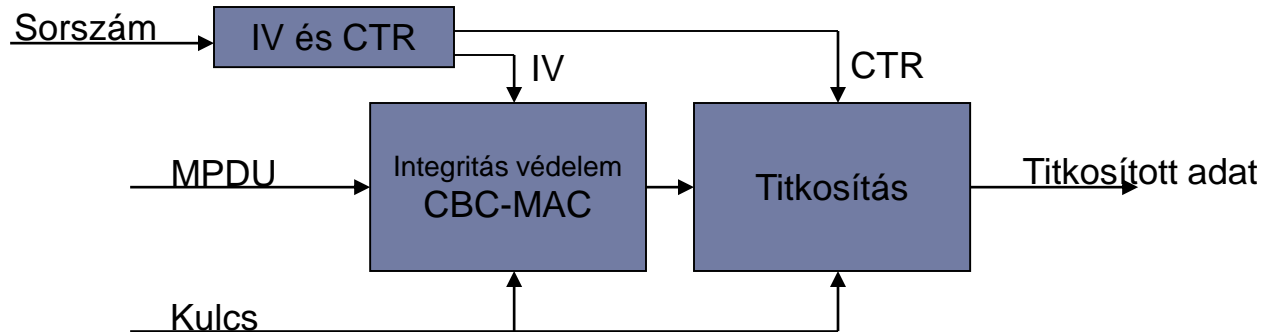


802.11i (WPA2)

- ▶ IEEE - 2004 –ben jelent meg
 - ▶ WPA +
 - ▶ Biztonságos IBSS
 - ▶ Biztonságos gyors hálózatváltások
 - ▶ A hitelesítés biztonságos feloldása
 - ▶ Új titkosító protokollok: AES-CCMP, WRAP
 - ▶ Már szükséges a HW módosítása is
 - ▶ Lassabb elterjedés, de mára már elterjedt

CCMP

- ▶ Counter Mode CBC-MAC Protocol
- ▶ Az AES használata



CBC-MAC

- ▶ Cipher Block Chaining Message Authentication Code
- ▶ Módszer
 - ▶ 1. Az első blokk titkosítása
 - ▶ 2. Az eredmény és a következő blokk XOR kapcsolat, aztán titkosítás
 - ▶ 3. A második lépés ismétlése
- ▶ Szükséges a kitöltés (padding)!

CCMP előnyök

- ▶ **Egyetlen kulcs elegendő**
 - ▶ Általában nem jó, ha ugyanazt a kulcsot használjuk, de itt nincs gond
- ▶ **AES előnyök**
 - ▶ Előre számolható
 - ▶ Párhuzamosítható
 - ▶ Nagy biztonság
- ▶ **Mentes a szabadalmaktól**

WLAN layer 2 védelem

	<i>WEP</i>	<i>TKIP</i>	<i>CCMP</i>
<i>Titkosító</i>	RC4, 40 vagy 104 bites kulcs	RC4, 128 és 64 bites kulcs	AES, 128 bites kulcs
<i>Kulcs élettartama</i>	24 bites IV	48 bites IV	48 bites IV
<i>Csomagkulcs</i>	Összefűzés	TKIP kulcskeverés	nem szükséges
<i>Fejléc integritása</i>	nincs védve	Michael: Forrás és cél MAC	CCM
<i>Adatok integritása</i>	CRC-32	Michael	CCM
<i>Visszajátzás védelem</i>	nincs védelem	IV szabályok	IV szabályok
<i>Kulcs-menedzsment</i>	nincs	IEEE 802.1X	IEEE 802.1X

WPA3

- ▶ 2018 januártól / június / októbertől
 - ▶ „individualized data encryption” a publikus WiFi hálózatokon
 - ▶ Opportunistic Wireless Encryption
 - ▶ „Simultaneous Authentication of Equals” leváltja a korábbi PSK kulcscserét
 - ▶ „Forward secrecy” a lezajlott kommunikáció védett az aktuális kommunikáció kompromittálásától
 - ▶ Kijelző nélküli készülékek biztonságos csatlakozása
 - ▶ 192 bites biztonság a nagyvállalatoknak

WPS – WiFi Protected Setup

WPS - Wi-Fi Protected Setup

- ▶ Cél, hogy az egyszerű felhasználó is biztonságosan tudja használni az WiFi routert (SOHO környezet, 2007)
 - ▶ PIN kódos
 - ▶ Belső: PIN kód a WiFi eszköz konfiguráló weblapján
 - ▶ Külső: PIN kód kívülről (nem igényel előzetes csatlakozást)
 - ▶ Nyomógombos (Push-Button-Connect)
 - ▶ Egyéb megoldások
- ▶ Kommunikáció EAP üzenetek segítségével
- ▶ Gondok a tervezésnél
 - ▶ PIN kód (7 számjegy + 1 ellenőrző) esetén a helyes kódot 2 félben ellenőrzi le az AP. Emiatt 10^7 helyett csak $10^4 + 10^3$ ellenőrzés kell.
 - ▶ Brute Force támadás, 0-3 mp per próbálkozás
 - ▶ A DH algoritmus miatt lassú
- ▶ Megoldás
 - ▶ Letiltjuk a WPS-t (nem biztos, hogy le lehet tiltani).
 - ▶ Lock down

WPS üzenetek

IEEE 802.11			
	Supplicant → AP	Authentication Request	802.11 Authentication
	Supplicant ← AP	Authentication Response	
	Supplicant → AP	Association Request	802.11 Association
	Supplicant ← AP	Association Response	
IEEE 802.11/EAP			
	Supplicant → AP	EAPOL-Start	EAP Initiation
	Supplicant ← AP	EAP-Request Identity	
	Supplicant → AP	EAP-Response Identity (Identity: "WFA-SimpleConfig-Registrar-1-0")	
IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: SimpleConfig (0x01)			
M1	Enrollee → Registrar	N1 Description PK _E	Diffie-Hellman Key Exchange
M2	Enrollee ← Registrar	N1 N2 Description PK _R Authenticator	
M3	Enrollee → Registrar	N2 E-Hash1 E-Hash2 Authenticator	
M4	Enrollee ← Registrar	N1 R-Hash1 R-Hash2 E _{KeyWrapKey} (R-S1) Authenticator	prove possession of 1 st half of PIN
M5	Enrollee → Registrar	N2 E _{KeyWrapKey} (E-S1) Authenticator	prove possession of 1 st half of PIN
M6	Enrollee ← Registrar	N1 E _{KeyWrapKey} (R-S2) Authenticator	prove possession of 2 nd half of PIN
M7	Enrollee → Registrar	N2 E _{KeyWrapKey} (E-S2 ConfigData) Authenticator	prove possession of 2 nd half of PIN, send AP configuration
M8	Enrollee ← Registrar	N1 E _{KeyWrapKey} (ConfigData) Authenticator	set AP configuration
Enrollee = AP Registrar = Supplicant = Client/Attacker PK _E = Diffie-Hellman Public Key Enrollee PK _R = Diffie-Hellman Public Key Registrar Authkey and KeyWrapKey are derived from the Diffie-Hellman shared key. Authenticator = HMAC _{Authkey} (last message current message) E _{KeyWrapKey} = Stuff encrypted with KeyWrapKey (AES-CBC)		PSK1 = first 128 bits of HMAC _{Authkey} (1 st half of PIN) PSK2 = first 128 bits of HMAC _{Authkey} (2 nd half of PIN) E-S1 = 128 random bits E-S2 = 128 random bits E-Hash1 = HMAC _{Authkey} (E-S1 PSK1 PK _E PK _R) E-Hash2 = HMAC _{Authkey} (E-S2 PSK2 PK _E PK _R) R-S1 = 128 random bits R-S2 = 128 random bits R-Hash1 = HMAC _{Authkey} (R-S1 PSK1 PK _E PK _R) R-Hash2 = HMAC _{Authkey} (R-S2 PSK2 PK _E PK _R)	

Captive portál

Védelem a felsőbb rétegekben

Captive portal

- ▶ Védelem a hálózati rétegben
 - ▶ Layer 2 védelem nélkül
- ▶ Hitelesítés web szerver segítségével
 - ▶ A felhasználó nyíltan hozzákapcsolódhat a hálózathoz, de kezdetben tűzfal zárja el külvilágtól
 - ▶ DHCPvel címet is szerezhethet
 - ▶ Az első böngészés kérése átirányítódik a szolgáltató lapjára, ahol hitelesítheti magát
 - ▶ A hitelesítő lap TLS védett
 - ▶ Sikeres hitelesítés esetén a tűzfalat felnyitják
 - ▶ A forgalmat a továbbiakban titkosítani kell!