WEP és WPA

PPKE, ITK
Csapodi Márton

IEEE 802 (1983)

A LAN (Local Area Network) szabványai

A 7 rétegű OSI modell alsó két rétegéről szólnak: Data Link Layer, Physical Layer

A Data Link Layer két alrétegre bomlik az IEEE 802 szerint:

- Logical Link Control (LLC): a Network Layer felé elrejti a konkrét hálózat típusát
- Media Access Control (MAC): függ a hálózat típusától (Ethernet vagy WLAN)

OSI (Open Systems Interconnection) modell emlékeztető:

3. (Network Layer): IP csomagok közlekednek a forrás és a cél között
2. (Data Link Layer): Pont-pont kapcsolat az eszközök és a hálózati csomópontok között. Címzés minden hálózati eszközre egyedi MAC (media access control) address alapján.
1. (Physical Layer): A jel fizikai átvitele a médiumon.

IEEE 802.11

A WLAN (Wireless Local Area Network) szabványai

- rádióhullám: 2.4-2.5 GHz (3.6 GHz, 5 GHz is)
- bitráta: 1-300 Mbit/s (Gbit/s is)
- hatótávolság: néhányszor 10m (de több 100km is lehet parabola antennával)

Wi-Fi: A szabványnak való megfelelést igazoló kereskedelmi márkajelzés

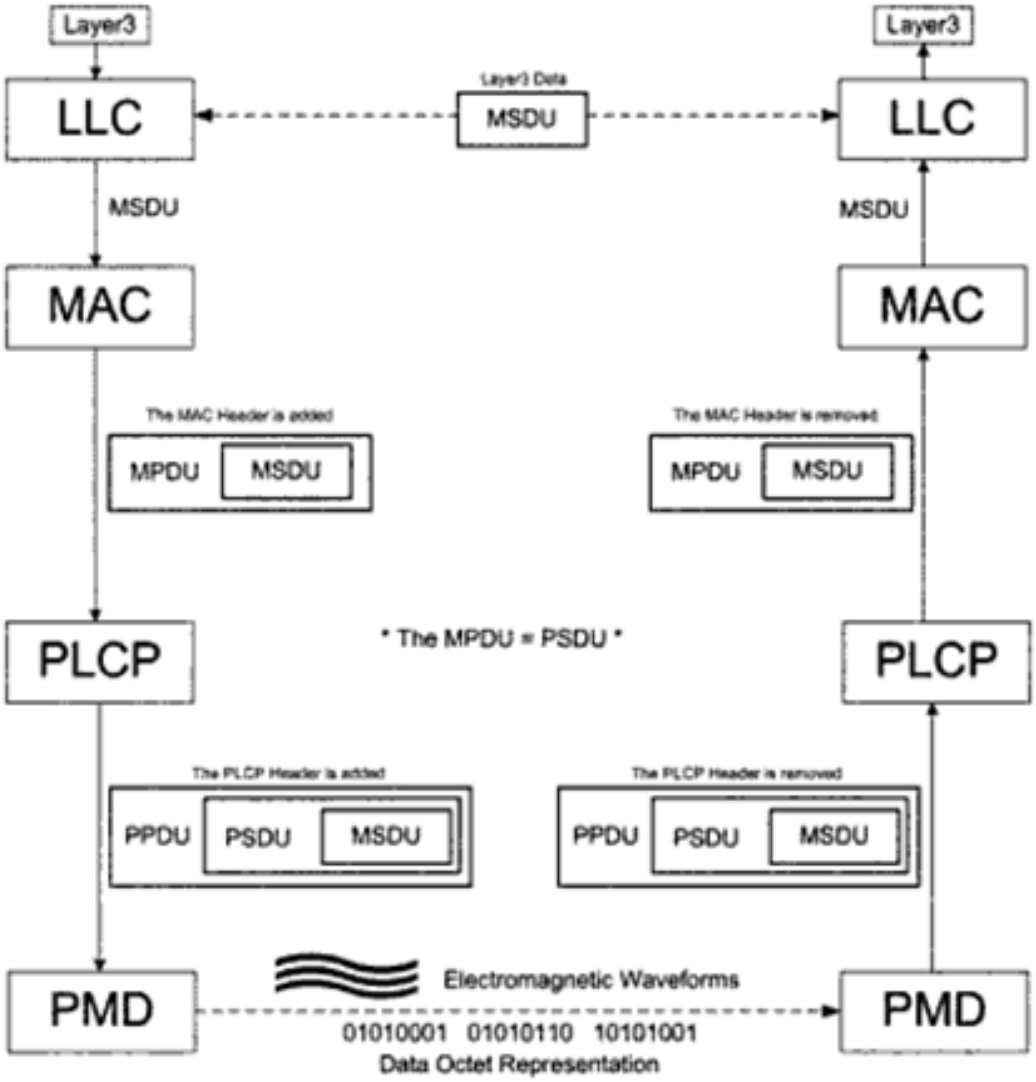
Az alap szabvány (1997, 1-2 Mbit/s) fontosabb kiegészítései:

- 802.11b: 10 Mbit/s-ig (1999)
- 802.11g: 54 Mbit/s-ig (2003)
- 802.11i: Enhanced Security (2004) - WPA2
- 802.11n: 600 Mbit/s-ig (2009)
- 802.11ad: 7 Gbit/s (2016) (új brand: WiGig)

WPA (Wi-Fi Protected Access) átmeneti megoldás volt a WPA2 szabvány elkészültéig

WLAN rétegek

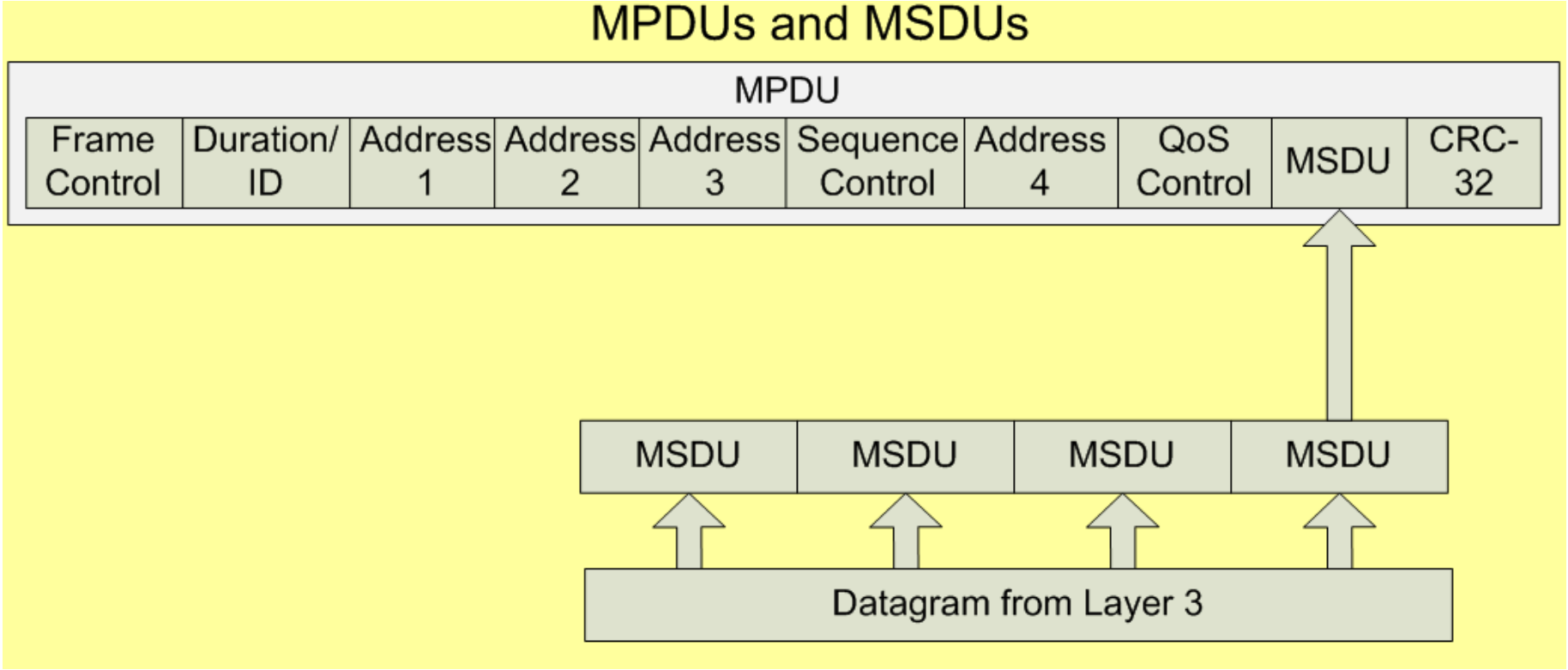
- MAC Service Data Unit (MSDU): Felette lévő OSI layerből kapott adat (pl. IP csomag), max.2304 byte-ra tördelve
- MAC Protocol Data Unit (MPDU): MSDU + header + ellenőrzőösszeg
- PLCP: Physical Layer Convergence Protocol
- PSDU: PLCP Service Data Unit (megegyezik az MPDU-val)
- PPDU: PLCP Protocol Data Unit
- PMD: Physical Medium Dependent



MAC üzenetcsomag

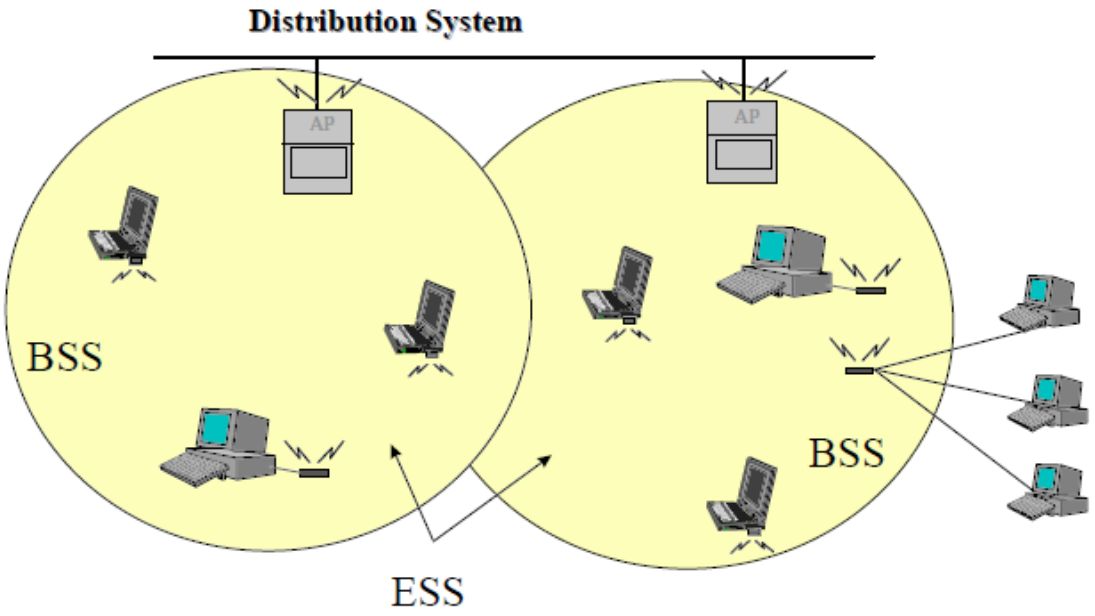
MSDU: titkosítás esetén ez megnő 8 byte-tal max. 2312 byte-ra

MAC Protocol Data Unit (MPDU): MSDU + header (max. 30 byte: 4x6 byte MAC address + 6 byte) + ellenőrzőösszeg (4 byte)



Tipikus WLAN

AP (Access Point): egy cellát kontrolláló bázisállomás
station: az AP-hez csatlakozó eszközök
BSS (Basic Service Set): egy AP és a csatlakozó eszközök együttese
BSSID (BSS Identifier): az adott BSS azonosítója (az AP MAC address-e)
IBSS (Independent BSS): ad-hoc hálózat, nincs kontrolláló AP
ESS (Extended Service Set): több BSS-ből áll, kifelé egy hálózatként látszik
SSID (Service Set Identifier):
egy vagy több AP-ból
álló WLAN azonosítója
Distribution System:
az AP-kat összekötő hálózat,
lehet Ethernet vagy wireless



Címmezők

4 címmező a kommunikáló eszközök és az irány függvényében

Frame Path	Address 1	Address 2	Address 3	Address 4
Frame between two wireless clients	Destination MAC	Source MAC	BSSID	N/A
Frame from network through AP to Client	Destination MAC	AP's MAC	Source MAC	N/A
Frame from client to network through AP	BSSID	Source MAC	Destination MAC	N/A
Frame traveling between two APs in a WDS	Receiving AP's MAC	Transmitting AP's MAC	Destination MAC	Source MAC

Frame típusok

Management Frame: access point broadcast üzenetek, autentikáció, kapcsolat létrehozása, átadása, bontása

Control Frame: Request to send, Clear to send (a csomagok egyszerre történő küldésének elkerülésére), Acknowledgement (hibamentes fogadás nyugtázása)

Data Frame: IP csomagokat szállít, csak ez kerülhet titkosításra, a többi nyílt

IEEE 802.11 biztonság

Az IEEE 802.11i kiegészítést megelőzően az alábbi lehetőségek léteztek:

	WEP Encryption	**No Encryption**
Open System Authentication	Encryption No Authentication	No Encryption No Authentication
Shared Key Authentication	Encryption Authentication	No Encryption Authentication

WEP: Wired Equivalent Privacy

IEEE 802.11 OSA

Nincs autentikáció.

Kölcsönösen elküldik a MAC address-t a kapcsolódás előtt.

Az AP-k lehetővé tesznek MAC address szűrést. Nincs értelme bekapcsolni, mert nehéz menedzselni összetett WLAN esetén, ráadásul a MAC address nyíltan közlekedik, lehallgatható és a támadó erre konfigurálhatja a hálózati kártyáját.

Az AP-k lehetővé teszik az SSID elrejtését. Nincs értelme bekapcsolni, mert ez is lehallgatható.

WEP titkosítás használható előre megosztott kulcs alapján. Ez valójában autentikációt is biztosít ezáltal. Biztonságosabb, mint a Shared Key Authentication

IEEE 802.11 SKA

Shared Key Authentication:

1. kliens kapcsolódni akar
2. access point 1024 bites véletlen challenge-et küld
3. kliens elküldi: IV, WEP([challenge,checksum], [IV,shared key])
4. access point dekódol, összevet, nyugtáz

IV: 24 bites kezdeti érték, kliens határozza meg

[challenge,checksum]: a kihívás és a CRC-32 összefűzve

[IV,shared key]: a kezdeti érték és a megosztott kulcs összefűzve

WEP(M, k): WEP algoritmussal, k kulccsal titkosított M adat

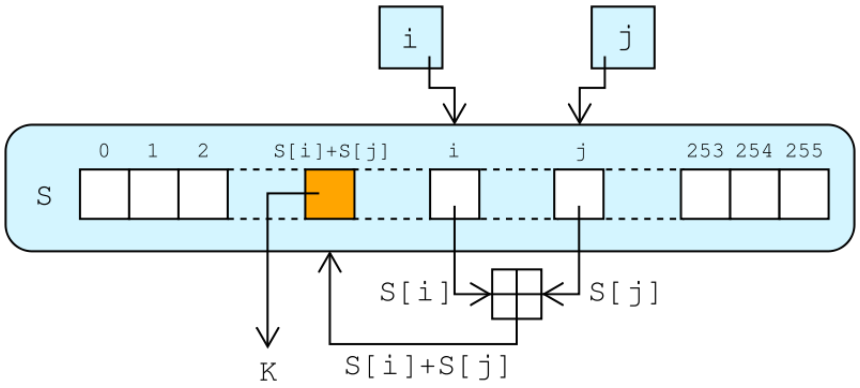
WEP - Wired Equivalent Privacy

Eredetileg 40 bit kulcs (5 karakter) + 24 bit IV (export korlátozások miatt)

Később 104 (13 karakter) + 24 bit IV is

RC4 algoritmus (64 vagy 128 bites kulccsal) a kulcsfolyam generálásra

Vernam rejtjelező (XOR)



WEP - SKA sérülékenység

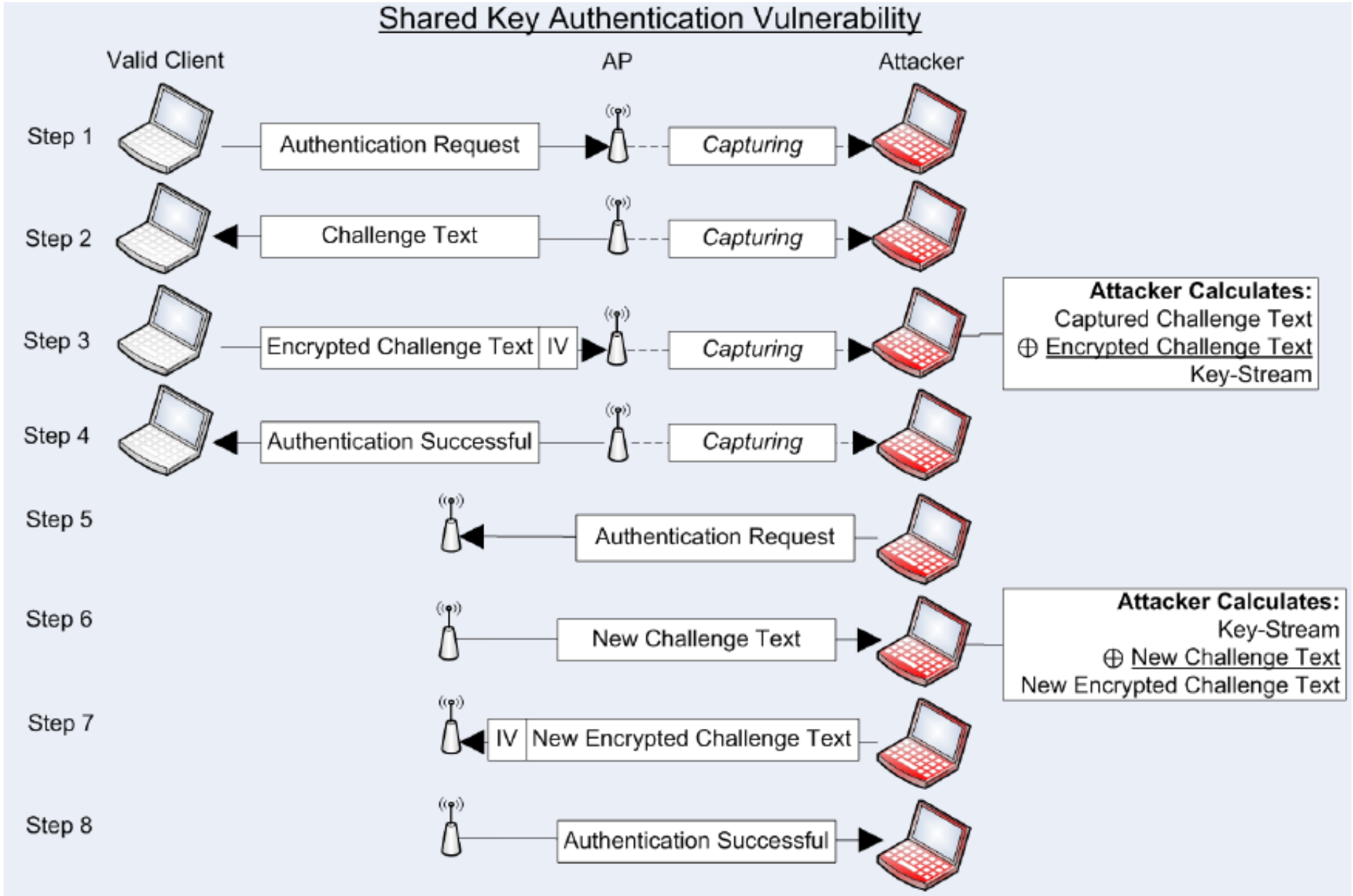
Autentikáció sérülékeny:

Challenge és WEP([challenge,checksum], [IV,shared key]) ismeretében a kulcsfolyam számítható a Vernam típusú adatfolyam-rejtjelező miatt. Ugyanazzal az IV-vel a támadó később autentikálhat.

A probléma abból ered, hogy a kliens határozza meg az IV-t és nyíltan küldi el.

Ha titkosítás is be van állítva, a támadó a sikeres autentikáció után sem tud kommunikálni.

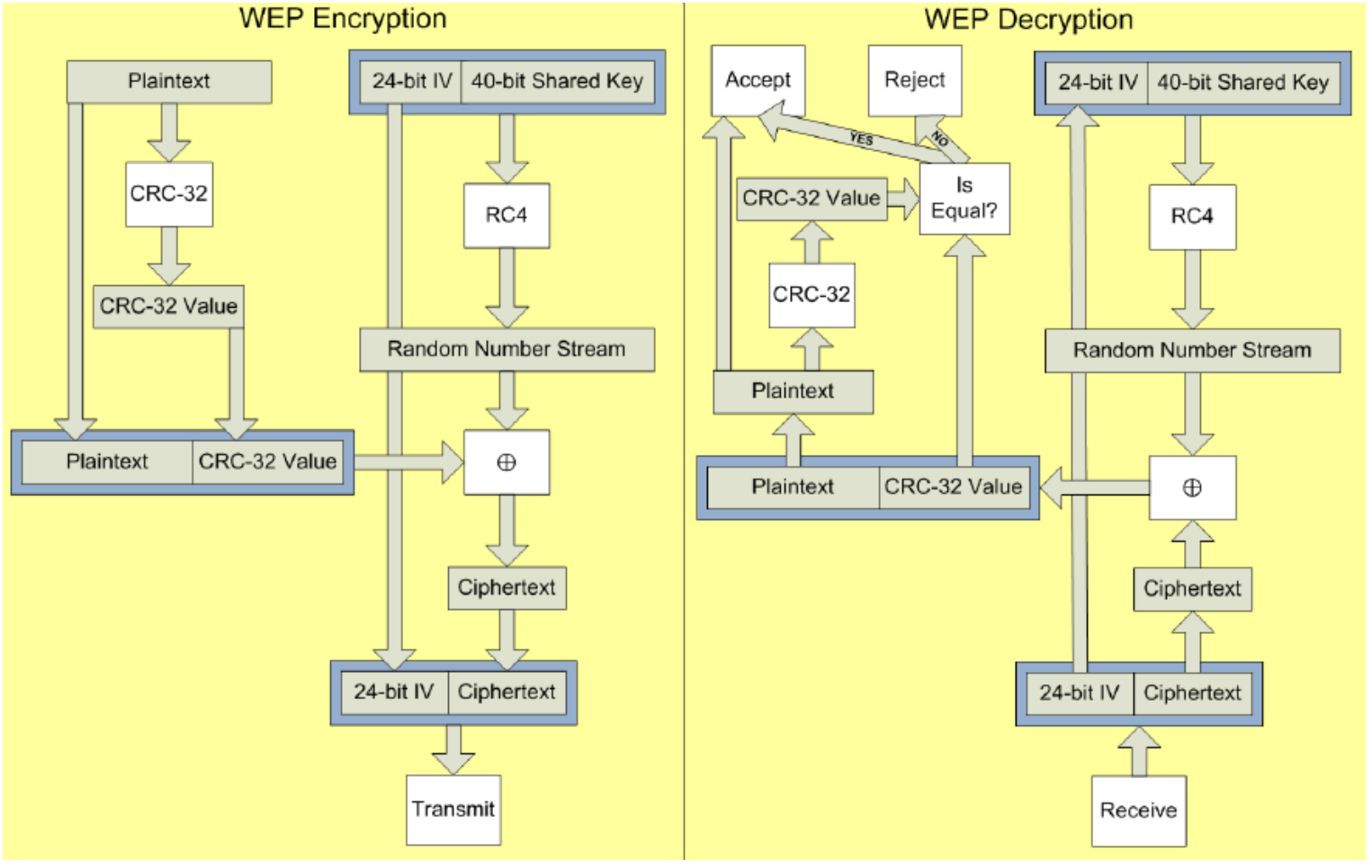
(Tilos használni az SKA-t titkosítás nélkül, mert nem biztosít autentikációt.)


Shared Key Authentication Vulnerability
Valid Client
AP
Attacker
Step 1
Authentication Request
Capturing
Step 2
Challenge Text
Capturing
Step 3
Encrypted Challenge Text
IV
Capturing
Attacker Calculates:
Captured Challenge Text
⊕ Encrypted Challenge Text
Key-Stream
Step 4
Authentication Successful
Capturing
Step 5
Authentication Request
Step 6
New Challenge Text
Attacker Calculates:
Key-Stream
⊕ New Challenge Text
New Encrypted Challenge Text
Step 7
IV
New Encrypted Challenge Text
Step 8
Authentication Successful

WEP rejtjelező

Szinkron üzemmódú adatfolyam rejtjelező: szinkronizálni kell, minden frame-nél újra indul -> kulcs változatlan, IV változik

Integritás védelem: 32 bites checksum



WEP - checksum sérülékeny

Érvényes ciphertext hozható létre a ciphertext módosításából.

Ha egy lehallgatott, érvényes ciphertext adat mezőjét megváltoztatjuk és az alábbi módon származtatjuk a módosított ciphertext-et:

C'=C XOR ([változás,CRC-32(változás)])

akkor a fogadó félnél az integritás ellenőrzés nem mutatja ki a módosítást.

Tetszőleges módon módosítható a ciphertext, a CRC-32 alapú integritásvédelem nem védi az integritást.

A probléma abból ered, hogy a CRC-32 leképezés és a Vernam rejtjelezés is lineáris függvény, így:

([M,CRC(M)] XOR K) XOR ([dM,CRC(dM)] = [(M XOR dM),CRC(M XOR dM)] XOR K

M: nyílt üzenet

dM: nyílt üzenet megváltozása

[M,CRC(M)]: összefűzött üzenet és ellenőrző összeg

WEP - IV ismétlődés

24 bites az IV

Születésnapi paradoxon: pár ezer frame-ben valószínűleg van két azonos IV

Azonos IV esetén megegyeznek a kulcsfolyamok, így a két ciphertext különbsége megegyezik a két cleartext különbségével.

WEP - frame beszúrás

DoS támadás intézhető egy érvényes MPDU üzenet ismétlésével.

Az AP elfogadja az üzenetet, mivel az IV véletlenszerű, így nem zárható ki az ismétlődés. Kicsomagolja és a tartalmát (MSDU) továbbadja a magasabb OSI rétegek felé.

WEP - kulcs management

A szabvány két kulcstípust tesz lehetővé:

- key mapping key: MAC address alapján egyedi kulcs minden kliensnek
- default key: amelyik MAC addresshez nem rendel az AP egyedi kulcsot, ez a default

Elvileg lehetséges volna minden kliensnek külön kulcsot adni és azt az AP-kben tárolni. De ez bonyolult. A gyakorlat az, hogy minden kliens ugyanazt a kulcsot használja:

- Akinek megvan a kulcs, minden kommunikációt dekódolni tud. Egymás üzeneteit dekódolni tudják a WLAN-on belül.
- Ha egy eszköz kompromittálódik vagy valaki kiadja másnak a kulcsot, idegen személy/eszköz is mindent le tud hallgatni.
- Ha megszűnik egy jogosultság (pl. kilépő dolgozó), cserélni kellene a kulcsot, de ez nem történik meg.

WEP - gyenge kulcs

A beállított jelszó nem 40, illetve 104 bit entrópiájú, így szótár alapú támadással kereshető.

(A 40 bites kulcs brute force módon is megkereshető.)

WEP - shared key felderítése az AP támadásával

ARP (Address resolution protocol): IP cím és MAC address között teremt kapcsolatot.

Mérete alapján felismerhető: mindig 42 vagy 60 byte

Fix 16 byte header: 8 byte LLC réteg header-je, 8 byte (kétféle: request v. reply) ARP header

A rejtjelezett frame első 16 byte-jából 16 byte key stream meghatározható.

A frame beszúrás támadás lehetővé teszi, hogy ugyanazt az ARP kérést számtalanszor elküldje a támadó, amire mindig új IV-vel kap választ, amiből mindig kinyerhető a 16 byte key stream.

Megfelelő mennyiségű key stream alapján a shared key megállapítható.

Szükséges idő: 1 perc (104 bites kulcsra)

WEP - shared key felderítése a kliens támadásával

Ehhez a támadáshoz nem kell az AP közelében lenni, csak a bekapcsolt kliens közelében.

A kliens állandóan poll-ozza az elérhető AP-ket.

A támadó lehallgatja az SSID-t és megszemélyesíti az AP-t: küld egy kihívást.

Kliens elküldi a titkosított kihívást.

AP visszaküldi, hogy "sikeres autentikáció"

Kliens újabb titkosított üzenetet küld.

Néhány óra alatt a 104 bites kulcs megfejtéséhez szükséges mennyiségű adat keletkezik.

IEEE 802.11i kiegészítés

Két új algoritmus:

WPA (Wi-Fi protected access): TKIP algoritmus (Temporal Key Integrity Protocol). RC4 a titkosító algoritmus, de IV és shared key keveredik, továbbá jobb az integritásvédelem.

WPA2: AES blokk rejtjelező CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) módban

Mindkettőnél:

Új kulcs hierarchia

Négy lépéses kölcsönös autentikáció

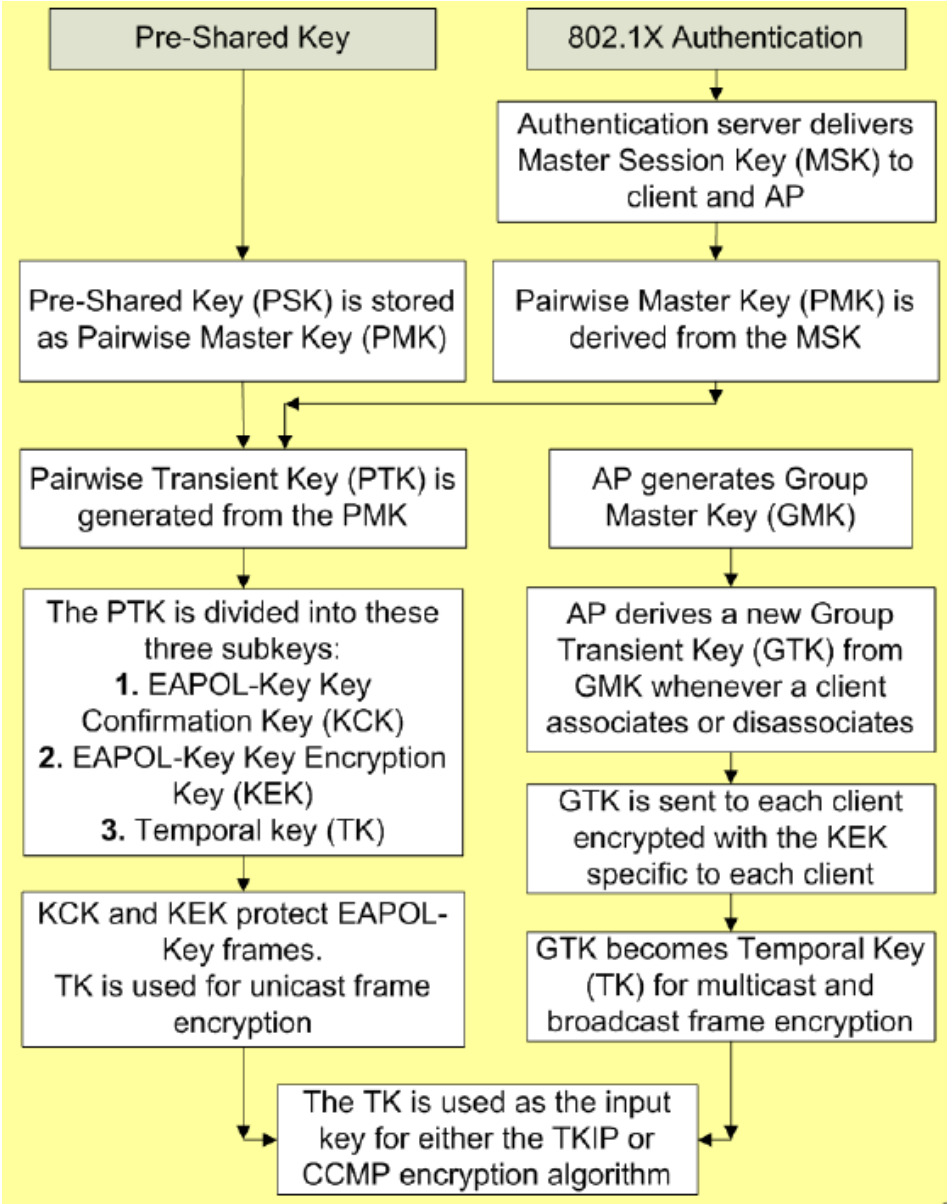
Előre megosztott kulcs vagy LAN hálózati hitelesítésből származtatott kulcs

IEEE 802.11i kulcs hierarchia

PMK: megosztott kulcsból (állandó) vagy LAN autentikációból (kliensenként és kapcsolódásonként különböző)

PTK: Kapcsolatonként eltérő akkor is, ha PMK fix. Ebből származnak a kapcsolat kulcsai.

GMK: Broadcast üzenetek közös kulcsa (ne kelljen n példányban kódolni). Minden kapcsolat bontáskor újra generálódik, így a kilépő kliens nem rendelkezik vele.



IEEE 802.11i handshake

Egyedi PTK létrehozása a PMK-ból, eszköz azonosítókból és mindkét fél véletlen számából.

GTK megküldése.

Kölcsönös hitelesítés.