Mérési útmutató az elektronikus kereskedelem biztonsága laboratórium (VIHI5317) méréseihez

Az IEEE 802.11i kapcsolat-felépítés vizsgálata – RADIUS alapú hitelesítés EAP-TLS módszerrel WLAN hálózatban

Mérés helye: Híradástechnikai tanszék
Mobil távközlési és informatikai laboratórium
IB. 113.

A mérést összeállította: Faigl Zoltán

2005

1. A mérés célja

A mérés célja gyakorlatban megismertetni a hallgatókkal az IEEE 802.11i szabványban definiált hitelesítési, kulcslétesítési módszereket.
Ismert, hogy a 802.11i az IEEE 802.1x hitelesítési framework-re és az EAP-ra (Extended Authentication Protocol) épül. Az EAP felett többféle hitelesítési módszert lehet választani, ezekből a hallgatók az EAP-TLS hitelesítést vizsgálják meg. A mérés végére megismerhetik, hogy miként kell felkonfigurálni az egyes résztvevőket ahhoz, hogy működjön a hitelesítés és kulcslétesítés, illetve hálózatmonitorozó program segítségével elemzik a protokoll tényleges működését.

2. A 802.11i protokoll működése

Az IEEE által kidolgozott és jóváhagyott szabvány lényegében egy protokoll (ajánlás) csomag a meglévő és a jövőbeni fizikai vezeték nélküli hálózatok biztonságának fokozására. Tartalma igen szerteágazó, a vezeték nélküli hálózatokban eddig nem alkalmazott hitelesítési metódusokat és kriptográfiai újdonságok sorát vonultatja fel:

- IEEE 802.1x (vezetékes hálózatokban alkalmazott hitelesítési eljárásokat foglalja keretbe)
- EAP, RADIUS, WPA
- RSN (Robust Security Network)

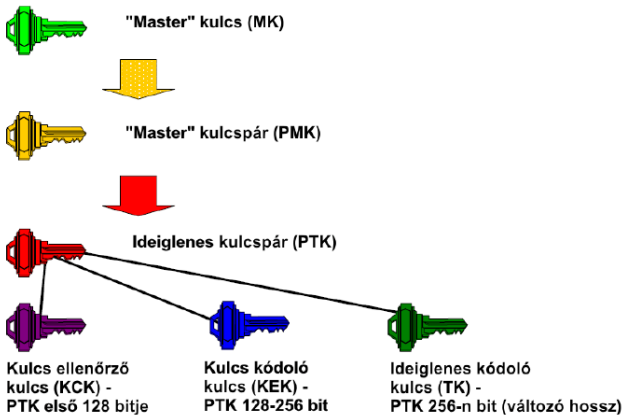
Új kriptográfiai eljárások:

- CCMP (AES - CCM), TKIP (Temporal Key Integrity Protocol)
- Dinamikus kulcs csere és management

A fő hangsúly a hálózati hitelesítésen és annak biztonságosságán van. Lényegében nem teljesen új átviteli protokollokat szabványosít a 802.11i, hanem meglévő, vezetékes környezetben korábban már széleskörűen alkalmazott eljárásokat implementál vezeték nélküli környezetbe.

2.1. Kulcs hierarchia

A 802.11i szabvány bevezetéséig mindössze egyetlen titkos kulcs létezett a hitelesítésre és az adattitkosításra. Az új eljárásokban kulcskezelési és generálási hierarchiát vezettek be, hogy megoldható legyen a kulcsok rendszeres időközönkénti cseréje, ami ellehetetleníti a lexikonépítő és egyéb, a hálózati forgalom lehallgatása és utána abból a kulcs kinyerésére irányuló támadási lehetőségeket. A kulcs hierarchia a következőképpen néz ki (1. ábra):



1. ábra IEEE 802.11i kulcshierarchia

Az 1. ábrán látható hierarchia képezi az új szabvány biztonságának alapját. A MK (Master Key) a legfelső titok, melyet mind a kliensnek, mind pedig a hitelesítést végző eszköznek ismernie kell. A PMK-t (Pairwise Master Key) a mobil állomás és a hitelesítő szerver (AS) minden egyes bejelentkezésnél a Master kulcsból generálja. A hitelesítő szerver ezt a kulcsot elküldi a klienssel kapcsolatban lévő APnak, mely ezután engedélyezi a 802.11 csatornán a kommunikációt. A PMK-ból 4-utas-kézfogással generál a kliens és az AP ideiglenes kulcsot (PTK).
Az ideiglenes kulcs (PTK – Pairwise Transient Key) a PMK-ból származik, minden bejelentkezéskor illetve minden frissítési kérelemnél újra generálódik. A PTK generálásához a kliens és az AP MAC címét, valamint az általuk generált két álvéletlen számot („nonce") használják. A PTK egy „kulcs csomag", mely tovább bontható kisebb csoportokra. Az első 128 (0-127) biten elhelyezkedő ún. kulcs ellenőrző kulcs (KCK – Key Confirmation Key) azt a célt szolgálja, hogy az AP és a kliens leellenőrizze, valóban ugyanazzal a PMK-val rendelkezik. Célja a kulcs meghamisításának megakadályozása. A kulcskódoló kulcs (KEK – Key Encryption Key) célja csoportos átmeneti kulcs (GTK – Group Transienk Key) titkosított kiosztása, melyet az AP küld a kliens felé.

A csoportos kulcsot multicast és broadcast üzenetek titkosítására használhatják az egy csoportban lévő állomások és az AP. A GTK kulcsot az AP generálja le és osztja szét. A GTK nem tartozik a Pairwise hierarchiába. A Pairwise kulcshierarchia a unicast kommunikációhoz tartozó kulcsok képzésére vonatkozik.

Az ideiglenes kódoló kulcs (Temporal Key) szolgálja az adatok kódolását, mely kódolás történhet RC4 vagy CCMP (AES-CCM – Advanced Encryption Standard – Counter Mode Encryption) algoritmusokkal. A 802.11i szabvány rugalmasnak tekinthető, mivel annak ellenére, hogy a CCMP bevezetése új hardver eszközök bevezetését követeli meg és ez nem valósítható meg korábbi hálózatokban, egyszerű driver frissítéssel (firmware) az összes 802.11i funkció elérhetővé válik az AP-ban, az AES-CCMP kivételével.

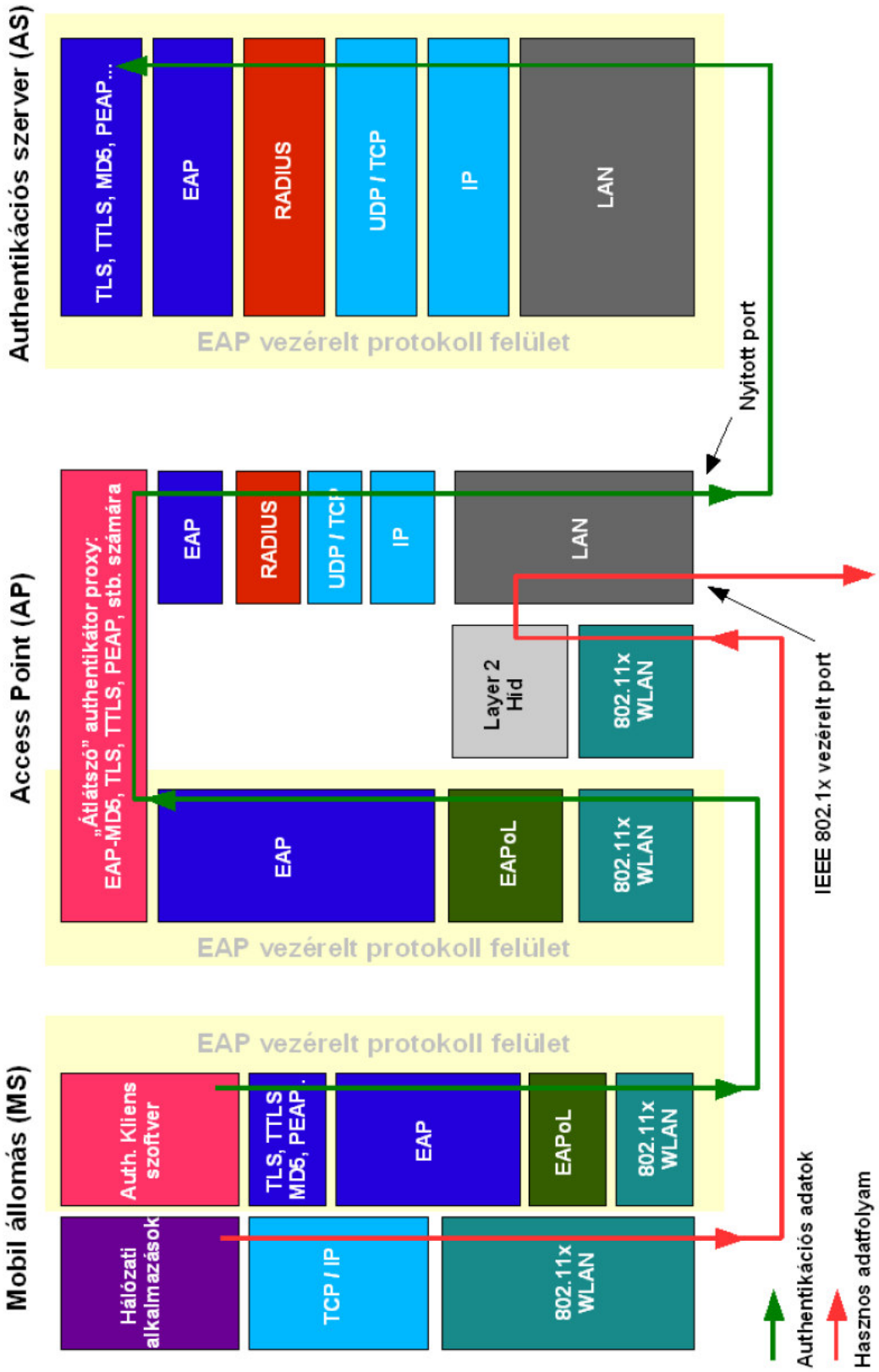
2.2. Protokollok a 802.11i szabványban

A IEEE 802.1x széles körűen elterjedt szabvány a vezetékes hálózatok körében. Az EAPot (Extensible Authentication Protocol, RFC 2284) és annak alváltozatait használja fel hitelesítési célra. A vezeték nélküli hálózatokban történő felhasználása a 802.11i elfogadásával vált általánossá. Az EAP nem egy hitelesítési protokoll, inkább egy, korábban a vezetékes hálózatokban már sikerrel alkalmazott adatátviteli technológia. A 802.1x az ún. Port-Based Network Access Control eljáráson alapul. Ez annyit jelent, hogy hitelesítés előtt nem tud kommunikálni a kliens az adott UDP/TCP porton, kivéve a hitelesítési szerverrel, sikeres azonosítás után viszont engedélyezetté válik a kommunikáció. A port megnyitása előtt EAP protokoll segítségével történik a kommunikáció. A WLAN hálózatban a kliens (Mobil Állomás) és a hitelesítési szerver EAP protokoll segítségével kommunikál. Az Access Point ebben a fázisban nem jut szerephez, tehát átlátszó proxy-ként kell viselkednie, át kell engednie a forgalmat a szerver felé és a szervertől a kliens irányába.
Az EAP független a hálózat más elemeitől, egyszerre többféle változata is tetszőlegesen használható hitelesítési célokra:

EAP-MD5: A RADIUS szerver a klienseket a felhasználó jelszavának MD5 ujjlenyomata alapján azonosítja. Ez a módszer nagyon egyszerű kevésbé erőforrás igényes, vezetékes környezetben elterjedten használt. WLAN esetben viszont nem ajánlott a használata, mert könnyen lehallgatható az MD5 hash.

LEAP (Lightweight EAP): Ezt az eljárást a Cisco cég dolgozta ki és használja eszközeiben. Hasonlóan az előzőhöz, MD5 lenyomatokat használ, viszont kétirányú azonosítást kíván meg (szerver és kliens oldalon egyaránt hitelesíteni kell egymást). WLAN eszközökben alkalmazott változata WEP kulcsok cseréjét is támogatja. Homogén, Cisco gyártmányú eszközökkel felépített hálózatban egyszerű lehet a használata, máshol viszont nem ajánlott a kompatibilitási problémák elkerülése végett.
EAP-TLS (Transport Layer Security): RFC 2716 szabvány. Kétirányú, szerver – kliens azonosítást használ, PKI kulcsinfrastruktúrán alapszik, X.509v3 tanúsítványokat használ a kliens és szerver publikus kulcsának hitelesítésére. A TLS az SSL-en (Secure Socket Layer) alapul, melyet elterjedten használnak a WEB-en titkosítás és hitelesítés céljából. A legtöbb kliens platformon (Linux, Windows, MacOS X) telepíthető kliens szoftver vagy modul. Több szoftverfejlesztő cég RADIUS szerverével (HP, Microsoft, FreeRADIUS.org, stb.) használható. Hátránya, hogy teljes nyílt kulcsú infrastruktúrát igényel (PKI – Public Key Infrastructure), melynek kidolgozása, a tanúsítványok, SMART-Card eszközök (a tanúsítványok egyénhez rendelése -és tárolására) beszerzése meglehetősen költséges. Ezzel szemben ez a módszer nyújtja a legnagyobb biztonságot hitelesítés tekintetében.
EAP-TTLS (Tunneled Transport Layer Security): Annyival egyszerűbb az EAPTLS- nél, hogy nincs szükség kliens oldali PKI infrastruktúrára, a kliens jelszóval azonosítja magát, tehát lecsökkenthetők a költségek. A szerver oldalon viszont továbbra is szükségesek a tanúsítványok.
PEAP (Protected EAP): Az EAP-TTLS és a PEAP között nincs működésbeli különbség, mindössze talán az, hogy a Microsoft és a Cisco áll e módszer mögött, ezért e cégek szoftvereiben (és hardver eszközeiben) ez a beépített funkció található meg.

A 2. ábra szemlélteti, hogy hogyan rétegződnek egymásra az egyes protokollok, hogyan folyik a kommunikáció. Az adatáramlás természetesen nem egyirányú, az ábra a hitelesítés irányát tűnteti fel zöld színű nyíllal, vörös színű nyíl segítéségével a felhasználói szinten lévő alkalmazás (pl. egy WEB-böngésző) kommunikációs útvonalát szemlélteti. Az EAP protokoll LAN hálózati interfészeken az ún. EAPoL (EAP over LAN) segítségével kommunikál. (2. ábra).



2. ábra: Az IEEE 802.1x protokoll implementációja WLAN hálózatra (WPA Enterprise)

A RADIUS (Remote Authentication Dial In User Service - RFC 2138) nem képezi szerves részét az új szabványnak. Az erre vonatkozó ajánlás fő célja az, hogy a vezetékes környezetben már bizonyított és jól bevált protokollt WLAN hálózatban alkalmazza. A RADIUS szerver

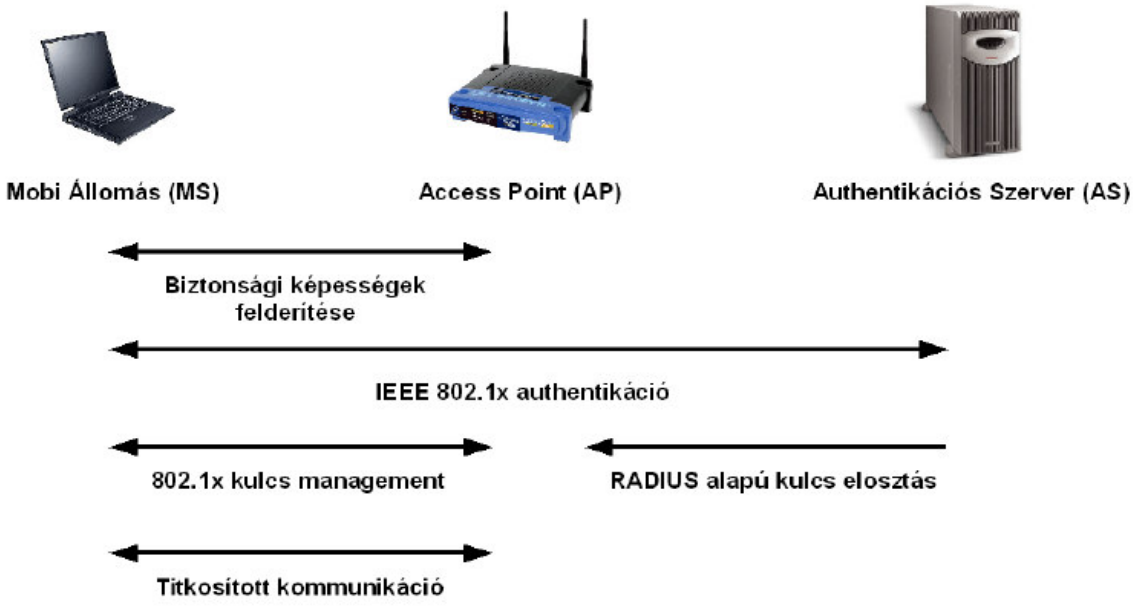
többféle adatbázist (LDAP, SQL variánsok, ORACLE stb.) támogat, melyben a felhasználó adatai (név, jelszó, kulcs, stb.) tárolódnak. Amennyiben az AP fel van készítve a RADIUS használatára, annak segítségével egyszerű, beágyazott (encapsulated) EAP üzeneteket továbbít és fogad az AS-től. (12. ábra) Négy ilyen üzenettípus lehetséges:

- Access-Request: AP → AS irányba, lekéredzés küldése
- Access-Challenge: AS → AP a szervertől visszajövő üzenet, Request elfogadása után
- Access-Accept: AS → AP sikeres hitelesítés esetén
- Access-Reject: AS → AP sikertelen hitelesítés esetén

A RADIUS üzenetváltásnál az AP és AS egy előre beállított statikus kulcs alapján MD5 hash-ek alkalmazásával kommunikál egymással.

2.3. Kommunikációs folyamatok

Miután bemutattuk, milyen kulcsokat és protokollokat használ a 802.11i szabvány, a kommunikációs folyamatok áttekintésével folytatjuk. (3. ábra). A biztonsági kapcsolat-felépítés három fő lépésből áll: képesség-felderítés, hitelesítés, kulcslétesítés. A negyedik fázis már magát a felhasználói adatok küldését jelenti az előre kiépített biztonsági alagúton.



3. ábra Az IEEE 802.11i biztonsági kommunikációs folyamatai

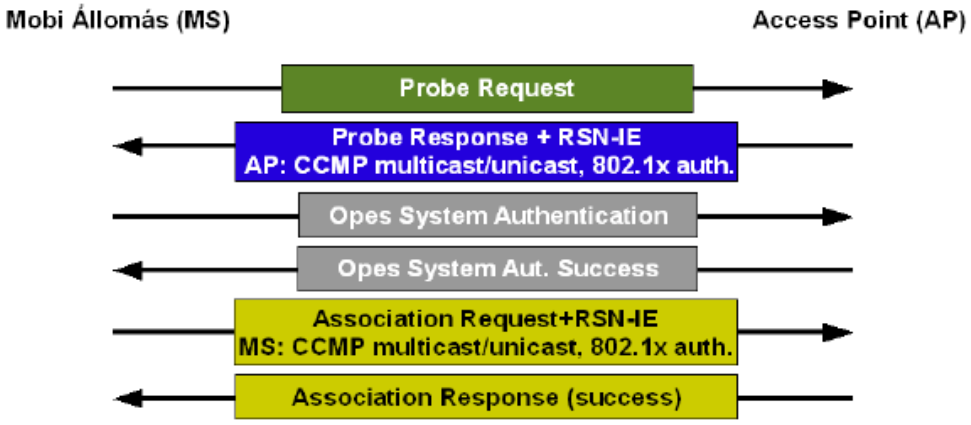
2.3.1. Biztonsági képességek felderítése

Az első lépésben a MS (Mobile Station) és az AP meghatározzák, milyen biztonsági beállításokkal rendelkeznek. Amikor a MS megtalál egy hálózatot (ha van SSID szórás, ha nincs a kézzel beállítottat keresi) egy Probe Request keretet küld. Az AP Probe Response kerettel válaszol. Ebben a csomagban található ún. RSN-IE (Robust Security Network - Information Element), amely a következőkről ad információt:

- AP hitelesítési képességei,
- Unicast (az MS és AP közötti, két szereplős kommunikációban) titkosítási beállítások,

- Multicast (egy küldő, több vevő) titkosítási beállítások.

A kommunikáló felek között lejátszódik az ún. IEEE 802.11 Open System Authentication. Ezt más néven MAC cím alapján történő hitelesítésnek is nevezhetjük, mely nem jelent mást, mint annak meghatározását, hogy az MS MAC címe szerepel-e az AP címlistájában. A MAC cím alapú hitelesítés nem közkedvelt a címlisták karbantartásának erőforrásigénye miatt. A visszafelé kompatibilitás megőrzése miatt építették be az új szabványba. Amennyiben ez a lehetőség nincs beállítva az AP-on, vagy a kliens MAC címe szerepel a listában, akkor az AP Open System Authentication - Success üzenettel válaszol. Ezután a kliens egy Association Request + RSN IE csomaggal válaszol, mely tartalmazza a MS képességeit, és a kérést, hogy ezekkel hozzáférhető-e a hálózat. Siker esetén az AP Association Response (success) üzenettel válaszol. A Probing-Authentication-Association fázisok az eredeti 802.11 WLAN szabványos kapcsolat-felépítési lépései. (4. ábra)



4. ábra Az IEEE 802.11i - Discovery folyamat

Az RSN-IE csomag egyik legfontosabb része az ún. Suite Selector (képesség kiválasztó). A Suite Selector tartalmazhat a szabványban meghatározott információkon kívül gyártóspecifikus információkat is. A szabványban meghatározott bináris-oktet üzenet tartalmak a következők lehetnek:

Hitelesítéss és kucs management funkciók lehetnek:

- 00:00:00:1 – 802.1X hitelesítés és kulcs management
- 00:00:00:2 – nincs hitelesítés, 802.1X kulcs management
- egyéb jelölések: gyártóspecifikus

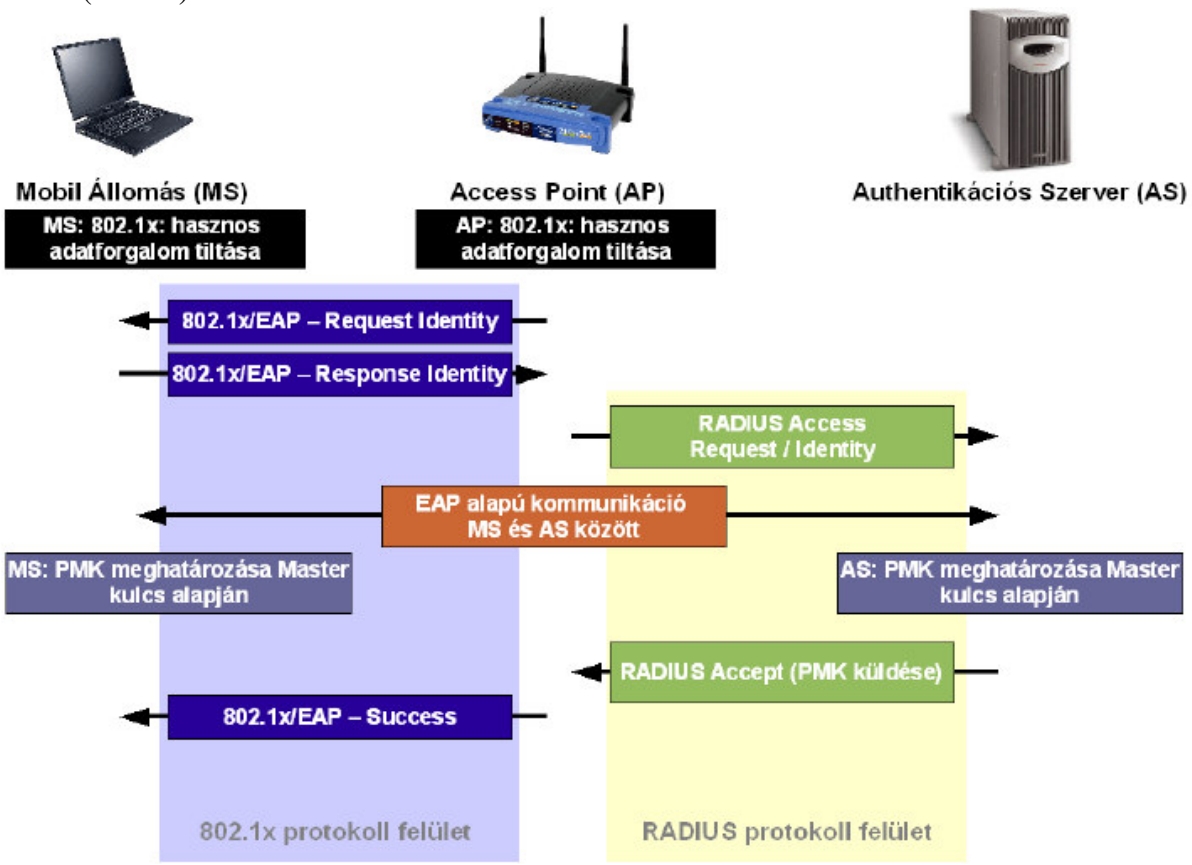
Kulcspár és titkosító funkciók lehetnek:

- 00:00:00:1 – WEP
- 00:00:00:2 – TKIP
- 00:00:00:3 – WRAP (Wireless Robust Authenticated Protocol)
- 00:00:00:4 – CCMP
- 00:00:00:5 – WEP-104 (WEP-104 bites kulccsal)
- egyéb jelölések: gyártóspecifikus

A biztonsági képességek felderítése során tehát a mobil állomás birtokába kerül az SSIDnek, a hálózatban használt hitelesítési és titkosító eljárásoknak. Az Access Point pedig tudja, hogy a használható képességek közül, a MS melyiket választotta.

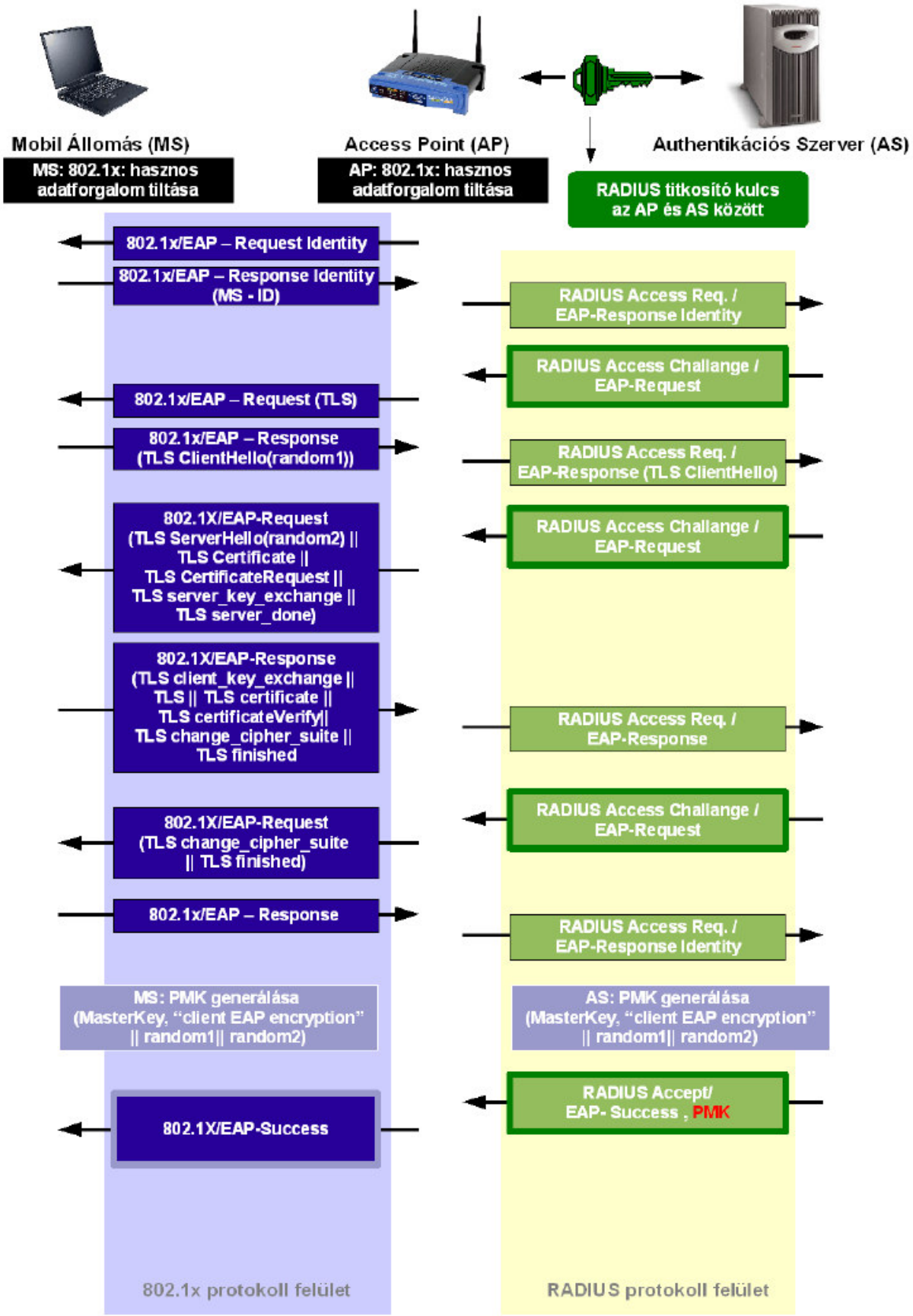
2.3.2. Az IEEE 802.1x hitelesítés folyamata WLAN hálózatban

A hitelesítési folyamat megkezdéséhez előzőleg sikeresen kiépített kapcsolatra van szükség az AP és a MS között. Ezen kívül rendelkeznie kell a kliensnek és a hitelesítést végző szervernek egy előzőleg megosztott kulccsal (ami lehet tanúsítvány, jelszó, stb.). Mivel az egyes kulcsok előállításához a MAC címre is szükség van, ezért ügyelni kell arra, hogy az Access Point és a Mobil Állomás ne rejtse el egymás elől a MAC címét.
A kommunikáció EAPoL és RADIUS csatornán történik. A hasznos adatforgalom TCP és UDP portjai a hitelesítési folyamatok idejére blokkolódnak, a 802.1x szabványban leírtak szerint. (5. ábra)



5. ábra Az IEEE 802.11i – EAP hitelesítési folyamat

Az hitelesítés folyamata a fenti ábrán látható. Miután az AP és a MS között létrejött a kommunikációs csatorna, az AP egy EAP-Request Identity üzenetet küld a MS felé. Sikeres válasz esetén az AP felveszi a kapcsolatot a RADIUS szerverrel, melyre bejelentkezik. Ezután az AP-nak nincs szerepe a kommunikációban, „átlátszó” proxy-ként átengedi a forgalmat a szerver és a Mobil Állomás között. Az MS és AS egyaránt rendelkezik a Master kulccsal (MK), melyből mindkettő létrehozza a PMK kulcsot. A RADIUS szerver a sikeres EAP kommunikáció után egy Accept üzenetet és az általa generált PMK kulcsot elküldi az Access Point-nak. Az AP sikeres üzenetvétel után egy EAP-Success üzenetet küld a MS felé. Az ábrán nem tűntettük fel az EAP típusát, mivel ez többféle lehet. Az IEEE 802.11i „de facto” szabványa az EAP típusára az EAP-TLS -t ajánlja. A 6. ábra az EAP-TLS alapú hitelesítés részleteit szemlélteti.



6. ábra Az IEEE 802.11i – EAP-TLS hitelesítési folyamat

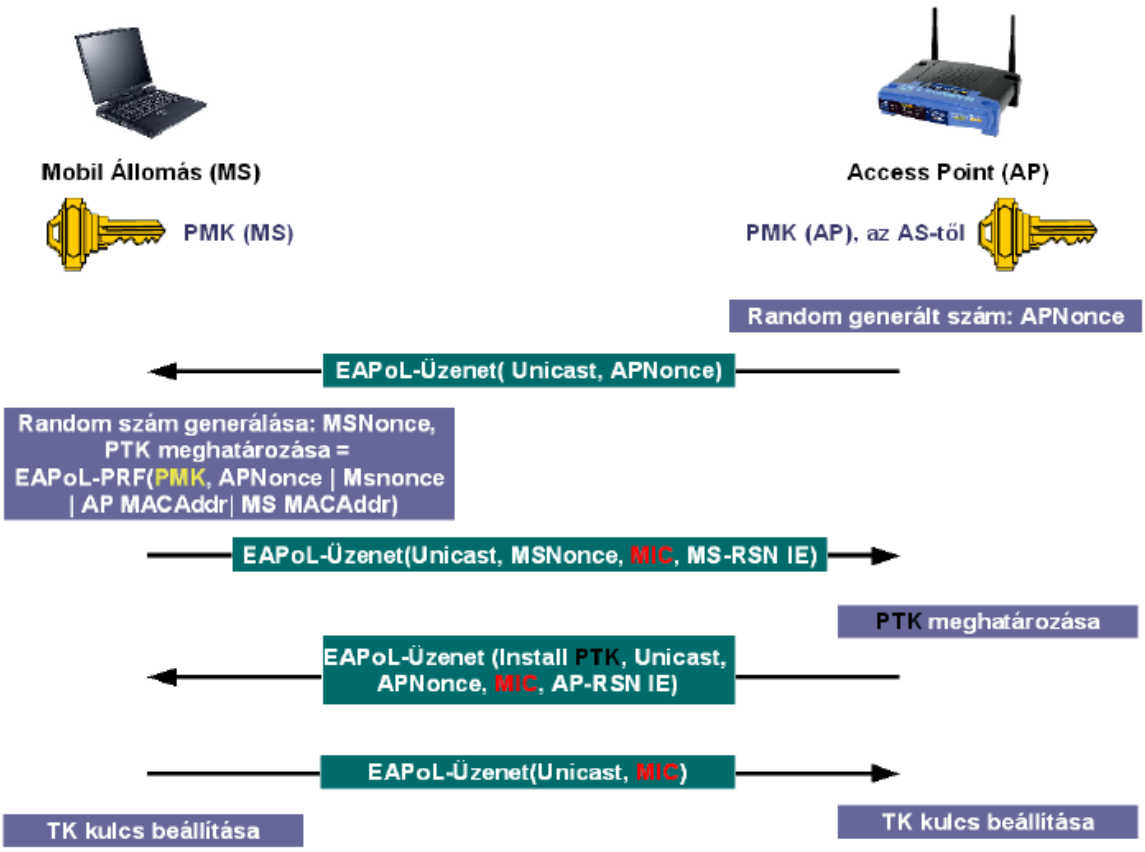
Az AP és AS megosztanak egy közös titkot, amelyet a köztük zajló üzenetek hitelesítésére használnak (HMAC-MD5 hash), illetve jelszó alapú hitelesítésnél a jelszó elfedésére (a jelszó HMAC-MD5 hash-kódját küldik át.
A kommunikációt ebben az esetben is az AP kezdeményezi egy EAP-Request Identity üzenettel, amire a Mobil Állomás egy EAP-Response Identity / MS-ID (MS-Identifier) üzenettel válaszol. Miután az AP észlelte, hogy EAPképes eszköz csatlakozott hozzá, kapcsolódik a RADIUS szerverhez (amely egyben TLS szerver is), elküld számára egy RADIUS Access Challange üzenetet, melybe be van ágyazva egy EAP-Response üzenet. A szervertől Access Challenge üzenet érkezik válaszul, melybe be van ágyazva az EAP-Request üzenet. Az AP ezt EAP-Request üzenet formájában továbbítja az MS felé.

Ha a felhasználó EAP-TLS hitelesítési módszert választott, és a szerver támogatja ezt, akkor az EAPoL és RADIUS üzenetekben TLS protokoll üzenetek kerülnek beágyazásra. A kliens és a szerver a tanúsítványok alapján hitelesítik egymást. TLS-hez szerver oldalon tárolni kell a szerver tanúsítványt és az ahhoz tartozó rootCA tanúsítványt, felhasználói oldalon tárolni kell a felhasználó tanásítványát és a rootCA tanúsítványát.

Sikeres hitelesítés után az AP és az AS is generál egy PMK kulcsot, majd az AS egy RADIUS Accept üzenetben elküldi az AP-nak a PMK kulcsot. Az AP a RADIUS Accept üzenetből tudja meg, hogy sikeres volt a szerver általi hitelesítés. Az AP EAP-Success üzenettel jelzi az állomásnak, hogy sikeres volt a hitelesítés. Ezután megnyitja a 802.1x controlled portot a kliens számára.

2.3.3. Kulcslétesítés

Az eredeti IEEE 802.1x szabványban lévő kulcs csere helyett egy újradolgozott kulcscserét használ a 802.11i (mivel az eredetit feltörték). A kulcslétesítés célja a PMK-ból PTK generálása az MS és az AP oldalán. A PTK generálásához a PMK-t és két random nonce-t használnak, az egyiket az MS, a másikat az AP szolgáltatja.
Az AP és a MS a PTK kulcs TK részét használja későbbiek során a felhasználói adatok titkosítására. Az üzenetek integritását az ún. MIC (Message Integrity Code - Michael) segítségével ellenőrzik kommunikáló felek. (7. ábra)



7. ábra „4 utas kézfogás” - kulcs csere a IEEE 802.11i szabványban

A PTK kulcs beállítása és verifikálása „4 utas kézfogás” segítségével történik (7. ábra). A folyamat a következőképpen játszódik le:

1. Az access point elküldi az általa generált véletlen számot (AP-nonce) a mobil állomásnak. A mobil állomás generál egy másik véletlen számot (MS-nonce). Ezután a a PMK, AP-Nonce, MS-nonce, AP MAC címe és a saját MAC címe segítségével legenerálja a PTK-t, az EAPoL-PRF (pseudo random function) függvénnyel.
2. Az AP egy EAPoL üzenetet fogad a felhasználótól, melyben megkapja a MS-nonce számot, és a mobil állomás RSN-IE üzenetét. Az RSN-IE-ből kiderül, hogy a mobil állomás milyen titkosító algoritmust szeretne majd alkalmazni a felhasználói adatok átvitele során. Az üzenet tartalmaz ezen kívül egy MIC (Message Integriti Code) kódot integritás-ellenőrzés céljából. Az AP szintén legenerálja a PTK kulcsot.
3. A harmadik lépésben az AP felszólítja a klienst a PTK használatára, az üzenet ezen kívül tartalmazza újra az APnonce véletlen számot, egy MIC kódot és az Access Point-által kiválasztott titkosító algoritmust (RSN-IE).
4. Az utolsó lépésben a Mobil Állomás egy EAPoL üzenettel válaszol az AP üzenetére, amely mindössze a MIC kódot tartalmazza. Ezután mindkét fél beállítja a PTK kulcs TK részét adattitkosítás céljára.

2.3.4. Adatküldés, titkosítási algoritmusok

A sikeres hitelesítés és kulcslétesítés után az IEEE 802.11i szabvány több módszert, algoritmust is biztosít a felhasználói adatok titkosítására.

- WRAP (Wireless Robust Authenticated Protocol)
- CCMP (Counter CBC-MAC Protocol)

- TKIP (Temporal Key Integrity Protocol)

Az 1. táblázat összefoglalja ezek jellemzőit:

	WEP	*TKIP*	*CCMP*
Kódoló algoritmus	RC4	RC4	AES
Kulcs mérete	40 vagy 104 bit	128 bit: kódolás, 64 bit: authentikáció	128 bit
Inicializáló vektor (IV)	24 bit hosszú	44+4 bit hosszú	44+4 bit hosszú
Adat integritás	CRC-32	MIC	CCM
Fejléc integritás	-	MIC	CCM
Ismétlés elleni védelem	-	IV vizsgálata	IV vizsgálata
Kulcs management	-	(EAP alapú)	EAP alapú

1. Táblázat: Titkosító algoritmusok és tulajdonságaik

Az új szabvány az WEP gyengeségeit felismerve a 24 bites IV helyett 48 bites IV-t használ (~16millió helyett, ~17,5×1012 állapot) mely esetén több mint 15 évig kellene várni, hogy megismétlődjön ugyanaz az IV, 54 Mbps adatsebesség és 1500bit-es csomagméret mellett. Az IV ugyan 48 bit hosszú, de az első 4 bitet ismétlés elleni védelmet szolgál. A nagyobb méretű IV és az ismétlés elleni védelem használatával kiküszöbölhető a „lexikonépítő" támadással történő kulcsszerzés. Mivel folyamatos a 802.11i bevezetése, ezért került a WEP kiegészítéseként a TKIP a szabványba. A TKIP használatához nem szükséges a meglévő hardver cseréje, mindössze a hardver meghajtó szoftverét (firmware) kell frissíteni mind AP és felhasználói oldalon. A TKIP továbbra is az RC4 titkosítást fogja használni, IV duplikáció nélkül. A TKIP algoritmus szétválasztja a titkosító kulcsot a hitelesítésnél használttal, a hitelesítés folyamata megegyezik a WEP-évél. A CCMP és a WRAP az AES különböző módozatait (OCB, CCM) használja titkosításra. Új hardver szükséges hozzájuk.

2.4. Hitelesítés előre osztott kulcsok alapján (WPA-PSK)

Kisebb hálózatokban felmerülhet a hitelesítési szerver (AS) elhagyásának lehetősége. A 802.11i szabvány erre az esetre is kínál lehetőséget, az ún. WPA-PSK (WPA - Pre Shared Key) megoldást. (8. ábra)

8. ábra A WPA-PSK működése

Valójában ez a megoldás nem hordoz magában 802.1x alapú (EAP) hitelesítési képességeket, tehát nincs EAP (EAPoL) és RADIUS protokoll alapú kommunikáció a két eszköz között. A

WPA-PSK mód általában mindegyik ma megvásárolható eszközön kiválasztható, vagy a régebbi WLAN eszközökhöz új firmware frissítéssel használhatóvá válik. Beállítása egyenként, minden eszközön külön-külön megadott jelszó vagy hexadecimális karaktersorozat (amely a PSK) segítségével történik. A PSK fogja reprezentálni ebben az esetben a RADIUS szervertől kapott PMK kulcsot. A felhasználói adatok titkosításához használt TK meghatározása az előzőekhez hasonló módon, „4 utas kézfogással" és véletlenszerűen generált (nonce) számok segítségével történik, azzal a különbséggel, hogy nem EAPoL üzenetekkel, hanem normál üzenetcsomagokkal (1500 bit) történik a kommunikáció. A PSK és az ebből generált kulcsok itt sem kerülnek átvitelre, a TK meghatározása után AES (CCMP, WRAP) vagy TKIP titkosító algoritmust használhatnak a felhasználói adatok titkosítására.
A WPA-PSK módszer használható Ad-Hoc hálózatokban is hitelesítés és adattitkosítás céljára (mivel Ad Hoc esetben nincs hitelesítést végző és a kommunikációt irányító kitüntetett fél).

2.5. Hitelesítési eljárások értékelése

Az hitelesítési eljárások értékelésekor a maximális biztonság és megbízhatóság mellett figyelembe kell venni az alkalmazott (vagy alkalmazni kívánt) környezetet, a WLAN hálózat kiterjedését (térbeli és fizikai), felhasználók változatosságát és maximális számát (nagy a felhasználók fluktuációja, avagy általában ugyanazok a felhasználók), az eszközök szabványoknak való megfelelését stb.
Biztonság szempontjából az eddigiek közül egyértelműen a IEEE 802.1x - EAP-TLS + CCMP a legjobb, mivel kétoldalú digitális tanúsítványokat használ a hitelesítésre, és az adattitkosítás is a legerősebb, AES algoritmussal történik. Az így megvalósított hálózatba történő illetéktelen behatolásra gyakorlatilag (és elméletileg sem) nem létezik módszer, viszont ennek kiépítése és fenntartása (PKI infrastruktúra, chipkártyák a tanúsítványok tárolására, hitelesítési szerver, legmodernebb WLAN eszközök, stb.) sok erőforrást igényel - pénzügyi és fizikai tekintetben egyaránt. Az ilyen hálózatokat csak nagyobb kiterjedésű, nagyvállalati vagy közigazgatási környezetben lehet hatékonyan realizálni.
Kisebb vagy közepes hálózatokhoz a PKI infrastruktúra elhagyásával jól használható és megfelelően hatékony biztonsági szempontból a IEEE 802.1x - PEAP vagy TTLS lehet. Ezekben a kliens oldalról egyszerűen, jelszó- és felhasználónév megadásával, mégis titkosított kommunikációval lehet hitelesítést megvalósítani. A PEAP viszont nem annyira biztonságos, mivel létezik a feltörésére megoldás. A kisebb, 2-4 Access Point-ot tartalmazó hálózatokban anyagi és strukturális szempontok miatt nem alkalmaznak külön hitelesítési szervert. Otthoni vagy kisebb, irodai (SOHO - Small office Or Home) hálózatokban nincs is általában szerver. Ebben a szituációban alkalmazható a WPA-PSK módszer, TKIP vagy AES titkosítással. Sajnos 2003. novembere óta ez sem teljesen biztonságos, ugyanis ekkor jelent meg először leírás a WPA-PSK módszerrel védett, TKIP algoritmussal titkosított hálózatok ellen alkalmazható támadásról. Azóta internetről szabadon letölthető alkalmazás is megjelent, mellyel komplett támadás indítható. Mivel a támadási módszer szótár alapú, „brute-force" ezért minél komplexebb és összetettebb megosztott közös kulcsok segítségével lehet egyedül védekezni ellene.
A legrégebb óta alkalmazott WEP (különböző változatai: 40, 104, 256 bit hosszú kulccsal) nyújtja a legalacsonyabb védelmet a támadásokkal szemben, számos alkalmazás létezik a feltörésére, ezért ennek használata egyáltalán nem ajánlott.
Az informatika területén 100%-os biztonság nem létezik, nincs védelem például durva behatolás (a hitelesítési szerver feltörése, adatok ellopása, cseréje) ellen, ezért a biztonsági szintek, hitelesítési metódusok megtervezésénél minél körültekintőbben kell eljárni, az alkalmazandó módszer(ek) tulajdonságainak, gyenge pontjainak feltérképezésével. A rendszer annyira lesz védve, amennyire a leggyengébb láncszeme biztonságos. Amennyiben hitelesítési

szervert használ a hálózat, akkor ez a kulcsfontosságú, hiszen ezen vannak a Master kulcsok, felhasználói adatok, a szerver hibája, kapcsolat megszakadása megbéníthatja az egész hálózatot. Másik járható út lehet a magasabb rétegek biztonságának fokozása. Ilyen lehet például az IPSec (Internet Protocol Security) vagy a VPN (Virtual Privte Netvork) alkalmazása.

3. Irodalomjegyzék

[1] Tóbi Tamás: „*WLAN authentikációs eljárások vizsgálata*”, Diplomaterv, BME-HIT, 2004

[2] C. Chaplin, E. Qi, H. Ptasinsky, J. Walker, S. Li: „*802.11i Overview*”, IEEE 802.11-04/0123r1, 2005 február

[3] Mick Bauer: „Securing your WLAN with WPA and FreeRADIUS, Part III.”, Linux Journal, http://www.linuxjournal.com/node/8151/, 2005 April

[4] Ken Roser: „HOWTO: EAP/TLS Setup for FreeRADIUS and Windows XP Supplicant”, http://www.freeradius.org/doc/EAPTLS.pdf , 2002 April

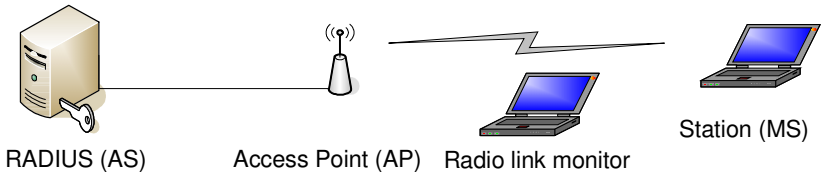
4. Ellenőrző kérdések

1. Milyen előzményei vannak annak, hogy EAP-TLS módszerrel működő RADIUS hitelesítést működtessünk? Melyik résztvevőnek milyen dolgokat kell támogatnia, milyen előzetes kulcsokkal kell rendelkezniük, milyen tanúsítványoknak kell meglenni a kliensnél és a szervernél?
2. Milyen főbb lépésekből áll a kapcsolat-felépítés 802.11i-nél?
3. Milyen hitelesítési módszereket és milyen titkosítási algoritmusokat támogat a 802.11i?
4. Milyen külső szabványokra épül a 802.11i? Azoknak mi a fő szerepük?

5. Mérési összeállítás

A mérés négy komponensből áll (9. ábra):

- MS: Portocom 5100C + 3Com SL-3040 PCMCIA-s kártya
- AP: Cisco 1100 Aironet AP (AIR-AP1121G-E-K9)
- RADIUS szerver: PC (Intel Celeron 600 MHz, 64MB RAM) + FreeRADIUS
- rádiós linket monitorozó számítógép: Compaq Series PP1020 notebook + Cisco AIR-PCM352 kártya



9. ábra: Mérési összeállítás

Az AS root jelszava: 6dr6w6dr6w. Belépés a méréshez: meres/6radius6
Az AP IP címe: 10.0.0.1, belépés webes interfészre: semmi / Cisco
A rádiós linket monitorozó gép root jelszava: 12345

6. Mérési feladatok

1. Állítsa össze a mérést és próbálja ki, hogy a kliens képes kapcsolódni az AP-hoz.

Kösse össze és kapcsolja be az AP-t és az AS-t! Kapcsolja be a kliens gépet is!

Ellenőrizze, hogy az AS IP címe 10.0.0.11.
Az AS-en root felhasználóként állítsa le a Radius szervert és indítsa el debug módban!

```
/etc/init.d/freeradius stop
freeradius -x
```

A szerveren indítson egy grafikus böngészőt és lépjen be az AP adminisztrátori felületére!

```
Cisco/Cisco vagy semmi/Cisco
```

A kliens gépen helyezze be a 3com kártyát, lépjen be a 3com utility-ba, ahonnan menedzselni tudja a vezetéknélküli kapcsolatokat! Adjon hozzá (vagy editáljon) egy kapcsolat-profilt, amelynél a következőket állítja be:

```
SSID: tsunami
Security type: WPA2, Authentication Type: EAP-TLS, Encryption Type: AES.
Client certificate: client smith (ez a kliens tanúsítványa)
Validate server certificate: Faigl Zoltán (ez a root CA tanúsítványa)
User Name: client smith (ő az, aki kapcsolódni szeretne)
Login Server: testserver (TLS szerver neve)
Az IP címet automatikusan kapja az AP-től!
```

Kapcsolódjon a klienssel az AP-hoz!

2. Tanúsítványok és szerver oldali beállítások vizsgálata.

Tanúsítványok meglétének és tartalmának vizsgálata:
Lépjen be a `/etc/freeradius/certs` könyvtárba. Talál ott egy `root.pem` és egy `crt-serv.pem` tanúsítványt.
Jelenítse meg őket!

```
openssl x509 -text -in root.pem
```

Melyik tanúsítványt ki adta ki, kinek adta ki? Melyik fájl tartalmaz privát kulcsot is?

A szerver tanúsítványnak (`crt-serv.pem`) van-e valamilyen kiterjesztett szerepe (ld `extended key usage` mező)?

Vizsgálja meg a kliensen a tanúsítványokat! `Vezérlőpult -> Internet beállítás -> Tartalom -> Tanúsítványok`
Keresse meg a személyes tanúsítványok között a `client smith` nevűt, és a legfelső szintű hatóság tanúsítványai között a `Faigl Zoltán` nevűt! Mi a kiterjesztett szerepe a client smith tanúsítványnak? Hányas számot talál ebben a mezőben?

A tanúsítványoknál melyik mező felelt meg a hálózatra történő belépés során a User Name-nek és a Login Server-nek?

Radius szerver beállításainak áttekintése:
Nézze meg a `/etc/freeradius/eap.conf` és a `radiusd.conf` fájlt a szerveren! Eszerint milyen hitelesítési módszereket támogat a freeradius?

Az EAP-TLS-nél milyen paramétereket kell konfigurálni, mi azok szerepe? Mire vonatkozik a jelszó?

Nézze meg a `clients.conf` fájlt a szerveren! Ez a fájl kiről szól, a felhasználókról vagy az Access Pointról?

Milyen beállítást talál a mérési összeállításra vonatkozóan a `clients.conf` fájlban?

Jogosultságok ellenőrzése:
Vizsgálja meg, hogy kik a tulajdonosai és milyen jogosultság attribútumok vannak beállítva a következő fájloknál ill. könyvtáraknál?

```
/etc/freeradius/
/etc/freeradius/eap.conf
/etc/freeradius/radiusd.conf
/etc/freeradius/clients.conf
/etc/freeradius/certs/
/etc/freeradius/certs/root.pem
/etc/freeradius/certs/serv-crt.pem
/etc/freeradius/certs/dh
/etc/freeradius/certs/random
/var/log/freeradius/
/var/log/freeradius/radius.log
/var/run/freeradius/
```

Vizsgálja meg, hogy milyen user nevén fut a freeradius, miután elindítottuk! Ehhez nézzen bele a radiusd.conf fájlba.

Miért voltak így beállítva a jogosultságok?

Milyen fő lépéseket tesz a freeradius indításkor? `freeradius -x` paranccsal debug üzemmódban indul. (Leállítás: `/etc/init.d/freeradius stop` vagy `CTRL-C` vagy `ps ax; kill radius_pid`)

Milyen fő lépések történnek a freeradius oldalán, amikor a client smith csatlakozik?

TLS szerver milyen kriptográfiai algoritmusokat támogat? `man ciphers`
Írja le, hogy milyen aláírási, titkosítási és hash-elő algoritmusokból válogatnak a TLS v1.0 cipher suite-ek!

Melyik cipher suite tűnik ezek közül a legerősebb és a leggyengébb kombinációnak?

3. **AP vizsgálata:**
   Lépjen be az AP management felületére a szerverről: `http://10.0.0.1 user: password: Cisco`
   Milyen beállítások láthatóak az AP-n, amelyek ahhoz szükségesek, hogy RADIUS alapú, EAP-TLS hitelesítés történjen, és WPA2-t (AES-CCMP titkosítást) követeljen elsősorban az AP?
   Ehhez nézze meg a következőket: `Security -> Encryption Manager, Security -> SSID Manager, Security -> Server Manager`

4. **Kapcsolat-felépítés lehallgatása.**

   Előkészületek

   Rádiós összeköttetés monitorozása:

   Kapcsolja be a monitorozó notebokkot! Bootoláskor válassza a `linux-bt6` kernelt! Lépjen be rootként! Helyezze be a Cisco kártyát! Ellenőrizze `iwconfig` paranccsal, hogy megjelent az eth0 és wifi0 interfész! Állítsa be a kártyát úgy, hogy ne kapcsolódjon semelyik AP-hoz sem a laborban! Ezt az `iwconfig eth0 essid none` paranccsal teheti meg. Ellenőrzésként újra beírhatja az `iwconfig` parancsot. Ezután rootként írja be a `kismet` parancsot! Ez egy hálózatmonitorozó program, amely monitor (promiscious) üzemmódba helyezi a kártyát. Ezután lépjen ki a kismetből (q és Shift-q). A kártya ettől monitor üzemmódban marad.
   Hálózatmonitorozó programként az Ethereal-t használjuk. Ezt grafikus felületen nyissa meg (`Alkalmazások-> Internet -> Ethereal`). A lehallgatáshoz menjen a `Capture->Interfaces` menübe. A megnyíló ablakban nyomjon a `wifi0` interfészhez tartozó `Prepare` gombra. Állítson be egy szűrőt, amely csak a klienstől és az AP-től jövő üzeneteket kapja el (`wlan host <AP_MAC> and wlan host <kliens_MAC>`) (Már ott lesz a szűrő). Érdemes bekapcsolni az `Update list packets in real time` checboxot. Ezek beállítása után elindíthatja a monitorozást a `Capture` gombbal.

   AS és AP közötti kommunikáció lehallgatása:

Indítsa el a szerveren rootként az Ethereal programot. Indítsa el a lehallgatást a Capture paranccsal.

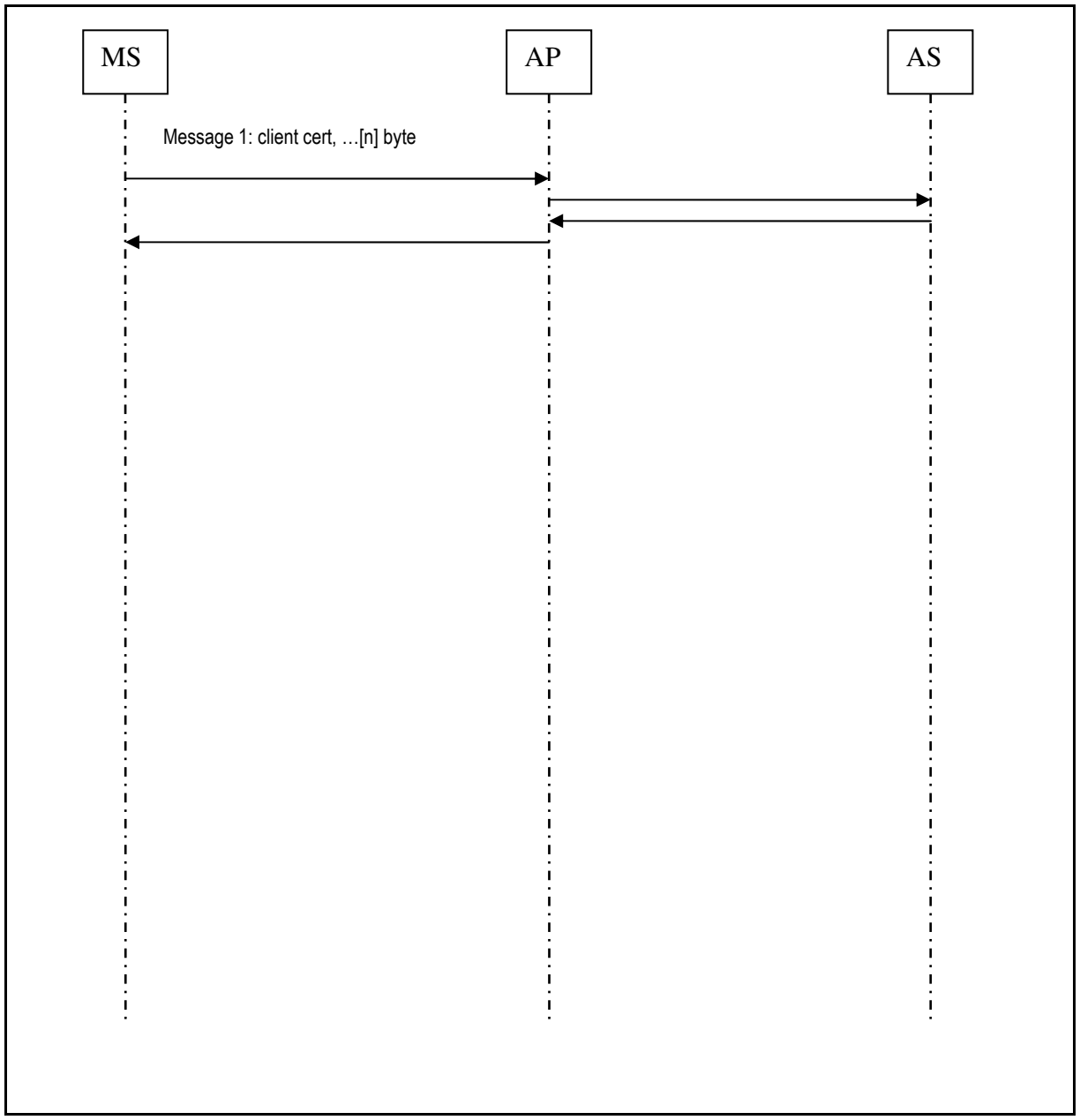
Mérés: A kapcsolat-felépítés üzeneteinek elkapása:

- Mielőtt elindítja a lehallgatást, a kliensen kapcsolódjon át az egyik `mcl` SSID-jű AP-ra.
- Indítsa el a monitorozást a szerveren és a monitorozó notebookon!
- Kapcsolódjon a klienssel az 1. feladatban beállított profillal az AP-hoz!
- Miután sikeresen kapcsolódott, állítsa le a monitorozást!

5. Mért eredmények elemzése:

Rajzolja az üzenetátvitel menetét a kliens – AP – RADIUS között egy üzenet-diagrammon! Jelölje a rajzon a következőket:

- Üzenet neve
- Az üzenetek hosszát
- Az üzenetekben a hitelesítés szempontjából fontos komponenseket. Mely üzenetekben mennek át tanúsítványok, cipher suite list, biztonsági-képesség információk, kulcs?



Mekkora időbe telik a sikeres kapcsolat-felépítés a lehallgatás alapján?

6. Protokoll működésének elemzése.

Meddig jut el a kapcsolat-felépítés, ha:

- Az AP és a kliens eltérő RSN IE-t támogat?

A Probing illetve Association során találhatjuk meg ezt a mezőt, amely megadja, hogy az AP milyen cipher suite-et (WEP, TKIP, AES-CCMP), illetve milyen hitelesítési típusokat (WPA- azaz 802.1x alapú hitelesítés stb.) támogat.

- AP-én nem engedélyezünk OpenAuhentication-t, pusztán EAP alapú hitelesítést? (AP-n állítsa be az SSID Settings-nél)?

- Rossz user nevet ad meg?

- Rossz szervernevet ad meg?