Debreceni Egyetem Informatikai Kar

Vezeték nélküli hálózatok biztonságának vizsgálata

Konzulensek:

Dr. Almási Béla
Egyetemi docens

Turi János
Cisco Systems Magyarország Kft.

Készítette:

Rózsa Gábor
Mérnök informatikus

Debrecen
2009

Tartalomjegyzék

Bevezetés

A kommunikáció és annak igénye egyidős az emberiséggel. Már a kisgyermek is kommunikál környezetével, igaz, ez még a kommunikáció kezdetleges formája. A kommunikáció általános jelentése a közlés, beszélgetés (információátadás), üzenetátadás. A kommunikáció az idők során sokat változott, és a mai világban egyvalamit biztosan megállapíthatunk: felgyorsult. Az emberiség az elmúlt évtizedektől kezdve különösen törekedett a kommunikáció hatékonyságának növelésére.

Ebben az évben – 2009-ben – az informatika szempontjából fontos évfordulóhoz értünk: 40 éves lett az Internet elődjének tekinthető ARPANET projekt. Az ARPANET projekt 1969 őszén jutott el abba a fázisba, hogy kézzel fogható eredményeket tudott felmutatni. 1969. október 29-én először küldtek üzenetet két hálózatba kötött számítógép között. A „login” üzenetből igaz, hogy csak a „lo” része ment át, de ez volt az első úttörő eredmény. A hálózatoknak számos előnyük van: erőforrás-megosztás, gyors és hatékony adatkommunikáció, leegyszerűsödő munkafolyamatok, terhelés elosztása, költségmegtakarítás, nagyobb megbízhatóság.

A kommunikáció alapvető elemei – adó, vevő, csatorna, üzenet – a vezeték nélküli kommunikációban is megjelennek: az adónak és a vevőnek a hálózathoz tartozó állomások felelnek meg, míg a csatornát a levegő jelenti. A számítógépes hálózatokon belül a vezeték nélküli hálózati kommunikáció nem sokkal több, mint 10 éves múltra tekint vissza. A vezeték nélküli hálózatok népszerűsége egyre nagyobb lett, ahogy fejlődött a technológia. Azonban sajnálatos módon a vezeték nélküli hálózatok biztonsága sokáig elmaradt a vezetékes hálózatok biztonságától.

Napjainkban az informatika hálózati részének legdinamikusabban fejlődő területei a biztonság, az IP alapú hangátvitel és a vezeték nélküli technológia. Amikor ez a három terület találkozik, számos kérdés, probléma merül fel. Ebből a három területből kettőt választottam dolgozatom témájául: a vezeték nélküli technológia biztonsági szempontjait.

A szakdolgozat két részre osztható: egyrészről bemutatom a vezeték nélküli hálózat elemeit és a használt technológiákat, protokollokat, szabványokat, másrészről a vezeték nélküli hálózat biztonságának gyakorlati vizsgálatát végzem el valós élethelyzetet szimulálva.

1. Vezeték nélküli hálózatok működési alapelveinek ismertetése

1.1. IEEE 802.11 szabvány

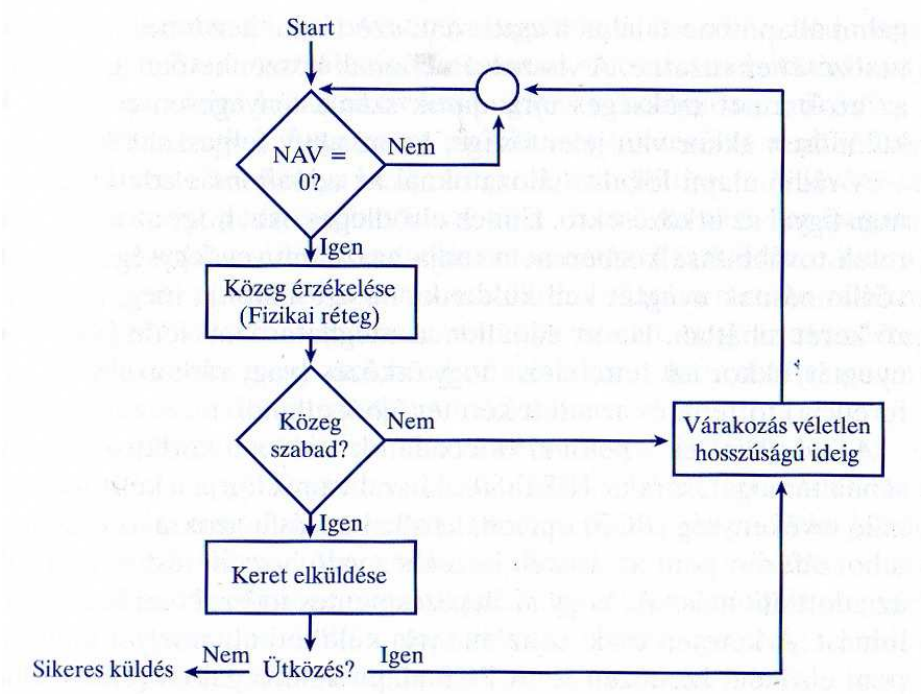
A hagyományos Ethernet hálózatokat az IEEE 802.3 szabvány definiálja, melyben minden kapcsolat egyértelműen rögzített körülmények között működik, így például adott a kapcsolat sebessége, duplexitása és az állapota. A vezeték nélküli hálózatoknak is van ilyen szabványa, ez pedig az IEEE 802.11. (Hucaby [2005] 435. old.) A 802.11 szabvány első változata 1997-ben jelent meg. Ez definiált egy általános közeghozzáférés-vezérlést (MAC) és számos fizikai réteget a vezeték nélküli LAN-okhoz[1]. A 802.11 munkacsoport jelenleg is fejleszti a szabványt, és újabb technológiákat dolgoznak ki a felmerülő problémák elhárítására és az új igények kielégítésére.

IEEE 802.11 MAC-réteg

A 802.11 szabvány egyetlen MAC-réteget specifikál, mely a 802.11 alapú hálózatok működését támogatja különböző funkciókkal. „A MAC-réteg a 802.11 állomások (rádiófrekvenciás hálózati interfészkártyák és hozzáférési pontok) között folyó kommunikációt az osztott levegőközeghez való hozzáférés koordinálásával irányítja és tartja fenn”. [Geier [2005] 124. old.] A 802.11 MAC-réteg – melyet gyakran tekintenek a hálózat agyának – irányítja valamely 802.11 fizikai réteg (pl. 802.11a) működését (átviteli közeg érzékelése; keretek küldése/fogadása). Mielőtt egy állomás keretet küldene, hozzá kell férnie a többi állomással közösen használt rádiócsatornához. A 802.11 WLAN-ok (vezeték nélküli helyi hálózatok) mindig fél-duplex üzemmódban működnek, mivel az állomások ugyanazt a frekvenciát használják adásra és vételre. Egyszerre csak egy állomás használhatja a közeget. A 802.11 szabvány két formáját adja meg a közeghozzáférésnek: az egyik az *elosztott koordináló tevékenység* (distributed coordination function, DCF), a másik a *kétpontos koordináló tevékenység* (point coordination function, PCF). A DCF alapja a kötelezően implementálandó CSMA/CA (vivőérzékelésen alapuló többszörös hozzáférés – Carrier Sense Multiple Access With Collision Avoidance). A DCF használatával az állomások versengenek a hozzáférésért és csak akkor próbálkoznak keretküldéssel, amikor már egyetlen állomás sem

[1] http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.std.html

végez adatátvitelt. Ha egy másik állomás keretet küld, akkor a többi állomás addig vár, míg szabad nem lesz a csatorna. (1. ábra)



1. ábra: A CSMA/CA működése.

Forrás: Geier [2005] 125. old.

A közeghozzáférés feltételeként a MAC-réteg megvizsgálja a hálózat allokációs vektor, a NAV (Network Allocation Vector) értékét, ami az előző keret elküldéséhez szükséges időt adja meg. Ezt az értéket minden állomásnál egy számláló adja meg és egy állomás csak akkor kezdhet el adni, ha a NAV értéke 0. A keret hosszát és az adatátviteli sebességet figyelembe véve az állomás adás előtt kiszámítja a keret küldéséhez szükséges időt, majd ezt az értéket beírja a keret fejrészébe, az időtartammezőbe. Az állomások, miután megkapták a keretet, ezen érték alapján kiszámítják saját NAV értéküket. Így biztosítható az adásban lévő állomás számára az átviteli közeg integritása. (Geier [2005])

A DCF a foglalt átviteli közeg vizsgálatához egy véletlenszerű visszaszámlálót tartalmaz (random back-off timer), melynek segítségével biztosítható, hogy ha felszabadul a csatorna, akkor nem kezd el minden állomás egyszerre adni. A rádió alapú vezeték nélküli hálózatoknál az állomások nem figyelnek az ütközésre az adatküldés során, mert az állomás nem tudja egyidejűleg használni a vevő- és az adóegységét. A vevőállomás ezért nyugtát küld, mellyel igazolja, hogy a keret hibátlanul megérkezett. Ha az adóállomás adott ideig nem kap nyugtát, akkor feltételezi, hogy hiba történt az átvitel során (ütközés, interferencia) és újraküldi az

adott keretet. A közeghozzáférés másik módja a kétpontos koordináló tevékenység (PCF), mely a 802.11 szabványban opcionális a DCF mellett. A legtöbb gyártó nem implementálja a PCF-et, mert a protokoll alkalmazása forgalomtöbblettel jár. (Roshan [2003]) A hozzáférési pont úgy engedélyezi a közeghozzáférést egy állomásnak, hogy ütközésmentes időszakban lekérdezi az állomást. Csak az az állomás küldheti el a kereteit, melyet elsőként kérdezett le a hozzáférési pont. (Geier, [2005])

MAC-réteg funkciói

Geier [2005] az alábbiakban foglalta össze az IEEE 802.11szabvány MAC-réteg funkciókat.

1. Letapogatás (Scanning)

A letapogatás az a folyamat, amikor a NIC (hálózati interfészkártya) hozzáférési pontokat keres. A letapogatás lehet: passzív és aktív. A passzív letapogatás során a NIC egyenként megvizsgálja a csatornákat a legerősebb jelű hozzáférési pont megtalálásához. A NIC a hozzáférési pontok által periodikusan sugárzott jelzőkeretek (beacon) segítségével vizsgálja meg az egyes jelek erősségét. A jelzőkeretekben a hozzáférési pont információi vannak (SSID, támogatott átviteli sebesség), és ezen információk, továbbá a jelerősség ismeretében az állomás össze tudja hasonlítani a hozzáférési pontokat. Aktív letapogatás során az állomás küld egy próbakeretet, melyre válaszolnak a hozzáférési pontok. A módszer előnye, hogy nem kell az állomásnak a jelzőkeretekre várnia, hanem kérheti a hozzáférési pontokat, hogy egy válaszkeretben küldjék meg az információkat, azonban ez többletforgalommal jár. Ad hoc üzemmódba állított állomások esetén az egyik állomás rendszeresen küld jelzőkeretet, mely figyelmezteti az új állomásokat a hálózat jelenlétére. A jelzőkeret elküldése fontos, mivel minden állomás megvárja a keretküldő periódus, illetve a véletlen hosszúságú visszatartó időzítő elteltét. Az állomás akkor kezd jelzőkeretet küldeni, ha ezen időtartamok alatt nem kap jelzőkeretet más állomásoktól.

2. Hitelesítés

A hitelesítés az azonosság bizonyítására irányuló folyamat (Geier [2005] 127. old.). Az IEEE 802.11 szabvány két változatát specifikálja a hitelesítésnek: a nyílt rendszerű és az osztott kulcsú hitelesítést. A hitelesítés folyamata és módszerei az 5. fejezetben kerülnek részletes tárgyalásra.

3. Társítás

A vezeték nélküli kapcsolat kialakításának következő állomása a társítás. Az állomásnak az adatkeretek küldése előtt asszociálnia (társulnia) kell a hozzáférési ponthoz. A folyamat során az állomás és a hozzáférési pont között fontos információk szinkronizálódnak, pl. átviteli sebesség. A társítást minden esetben az állomás kezdeményezi egy társítást kérő kerettel (association request frame), melyre a hozzáférési pont egy válaszkeretet (association response frame) küld. A társítás végeztével a hozzáférési pont regisztrálja az állomás adatait (pl. MAC-címét) és elkezdődhet az adatátvitel.

4. WEP

Amennyiben az opcionális WEP engedélyezve van, a NIC egy közös, egyeztetett kulccsal elküldés előtt titkosítja a keretek törzsét. A vevőállomás ugyanezzel a kulccsal visszafejti a keretet. A WEP biztonsági problémáit és a titkosítás kérdését a 4. fejezetben részletes tárgyalom.

5. Energiatakarékos mód

Ezen – a felhasználó által engedélyezhető – mód segítségével, a NIC úgy csökkenti a fogyasztást, hogy minden egyes keretben – egy a keret fejrészében található állapotbit beállításával – jelzi a hozzáférési pont felé, hogy alvó üzemmódba kíván kapcsolni és nem akar adatot küldeni. A hozzáférési pont minden alvó üzemmódban lévő hálózati kártya kereteit puffereli. Annak érdekében, hogy adatokat tudjon fogadni a NIC, periodikusan fel kell ébrednie, így fogadni tudja a jelzőkereteket. Ezekben a keretekben jelzi a hozzáférési pont, hogy vannak-e pufferelt, továbbításra váró keretek. A pufferelt keretek fogadása után a hálózati kártya visszatérhet alvó üzemmódba.

6. Darabolás

Az opcionális darabolás funkcióval elkerülhető egy esetleges interferencia esetén az újraküldés úgy, hogy az állomás az adatcsomagot kisebb keretekre darabolja. Az interferencia folytán fellépő bithibák nagyobb eséllyel csak egy-egy keretet fognak befolyásolni, mint az egész csomagot, így elég csak azt a keretet újraküldeni.

1.2. WLAN topológiák

„A 802.11 hálózatok tervezés szempontjából flexibilisek. Három lehetőségünk van WLAN topológiák kialakításakor (Roshan–Leary [2003] 39. old.):

- Független alap szolgáltatáskészlet (Independent Basic Service Set, IBSS)
- Alap szolgáltatáskészlet (Basic Service Set, BSS)
- Kiterjesztett szolgáltatáskészlet (Extended Service Set, ESS)"

„A szolgáltatási készlet alatt eszközök egy logikai csoportját értjük." (Roshan–Leary [2003] 39. old.) A vezeték nélküli LAN-ok esetében a jelek szórással továbbítódnak a rádiófrekvencián, ebből kifolyólag egy fogadó állomás több adó (pl. hozzáférési pont, jelismétlő) körzetében is lehet. Az adók a szolgáltatáskészlet azonosítóval, más néven SSID-val (Service Set Identifier) határozzák meg, hogy mely eszközöknek sugároznak.

Az **IBSS** egymással közvetlenül kommunikáló 802.11 állomások csoportja. Az így kialakult hálózatot gyakran hívják ad hoc hálózatnak, mert tulajdonképpen egy egyszerű peer-to-peer (P2P) WLAN. Ilyen hálózat akkor jön létre, amikor eszközök önállóan olyan hálózatot alkotnak, melynek csak ők a tagjai. A hálózatban nem vesz részt hozzáférési pont ezért ezt a szolgáltatási készletet függetlennek nevezzük. Az IBSS hálózatokra jellemző, hogy semmilyen előzetes felmérés (site survey) nem készül a létrejöttük előtt, és rövidebb ideig használják őket: pl. míg a szükséges információkat megosztják a résztvevők. Egy IBSS hálózat esetében nincs a szabványban maximalizálva a résztvevők száma. A **BSS** egymással kommunikáló 802.11 állomások csoportja, melynek középpontja a hozzáférési pont (AP). Az eszközön keresztül kommunikálnak, nem pedig közvetlenül egymással, ahogyan azt az IBSS hálózatokban teszik. A hozzáférési pontnak lehet egy ún. uplink portja (tipikusan nagy sebességű port a gerinchálózat irányába), mely a vezetékes hálózathoz csatlakoztatja a BSS-t. Az uplink interfészeken keresztül több BSS-t is össze lehet kapcsolni. A 802.11 terminológia szerint az uplink port olyan interfész, mely a BSS-t az elosztási rendszerhez (distribution system, DS) csatlakoztatja. A DS-en keresztül összekapcsolt BSS rendszereket **ESS**-nek nevezzük. A DS-hez csatlakozó uplink port lehet vezeték nélküli kapcsolat is, nem csak vezetékes, de a legtöbb esetben vezetékes portot használnak (Roshan – Leary [2003]).

1.3. Modulációs technikák

„A moduláció a hálózati adatokból olyan rádióhullámú jeleket vagy fényjeleket állít elő, melyek alkalmasak a levegőben történő továbbításra.” (Geier [2005] 89. old.) Moduláció során az információs jelet egy meghatározott frekvenciájú vivőjelre ültetik, így az információ a vivőn utazik, melyet a moduláló jellel az információt reprezentáló módon változtatják. A modulátor a forrásinformáció jelét egyesíti a vivőjellel. Az adóvevő a modulált és felerősített jelet az antennának továbbítja, ami a levegőben terjed tovább. Ezután a vevőegység antennája a demodulátorhoz továbbítja a vett jelet, ami az információs jelet leválasztja a rádiófrekvenciás vivőről (Geier [2005]).

Frekvenciabillentyűzés

Frekvenciabillentyűzés (FSK, Frequency Shift-Keying) során a vivőjel frekvenciájában kis változásokat idéznek elő, így téve lehetővé az információ reprezentálását. A moduláció az 1 és 0 adatbitet a vivő frekvenciájának pozitív vagy negatív eltolásával reprezentálhatja (pl. negatív eltolás esetén alacsonyabb frekvenciája lesz a vivőjelnek, így ábrázolva a logikai 0-át) (Geier [2005]).

Fázisbillentyűzés

Fázisbillentyűzéses modulációnál (PSK, Phase Shift-Keying) a jel fázisában idéznek elő változásokat, miközben a jel frekvenciája állandó marad. A fáziseltolás a frekvenciaponthoz viszonyított, meghatározott nagyságú pozitív vagy negatív érték lehet (Geier [2005]).

Kvadratúra-amplitúdómoduláció

Kvadratúra-amplitúdómoduláció (QAM, Quadrature Amplitude Modulation) esetében a vivőjelnek az amplitúdóját és a fázisát is megváltoztatjuk, így reprezentálva a szimbólumokat. Ezen moduláció előnye, hogy ezekkel a szimbólumokkal több bitből álló bitcsoportot reprezentálhatunk. „Egyes QAM technikát alkalmazó rendszerek 64 különböző amplitúdó-fázis kombinációt használnak, így szimbólumonként 6 bit reprezentálható. Néhány szabvány esetében (pl. IEEE 802.11a, IEEE 802.11g) a QAM révén nagyobb adatátviteli sebesség válik elérhetővé.” (Geier [2005] 92. old.)

Szórt spektrum

A digitális jelek FSK, PSK vagy QAM technikákkal analóg vivőjelekké történő modulálásán kívül egyes WLAN-ok a modulált jelet széles frekvenciatartományban terítik szét, melyet szórt spektrumnak neveznek. „Ez a módszer jelentősen csökkenti a ki- és befelé irányuló interferencia kialakulásának lehetőségét. ” (Geier [2005] 92. old.) A szórt spektrum a jel teljesítményét szétteríti egy széles frekvenciasávban, és az RF egységek a jel szétterítését közvetlen sorozat, vagy frekvenciaugrások formájában valósítják meg. A DSSS (közvetlen sorozatú szórt spektrum) az RF vivőjelet olyan digitális kóddal modulálja, melynek bitsebessége lényegesen nagyobb, mint az információs jel sávszélessége. FHSS alkalmazásánál (frekvenciaugrásos szórt spektrum) az RF vivőjel a meghatározott frekvenciatartományon belül különböző frekvenciaértékek között ugrál. A szórt spektrumú rendszerek többsége ipari, tudományos és orvosi célokat szolgáló (ISM), nem engedélyköteles sávokban működik (902 MHz, 2,4 GHz, 5,7 GHz), melyeket az FCC 1975-ben engedélyezett a WLAN-ok számára. Az ISM sávokat használó RF rendszereknek kötelező a szórt spektrum alkalmazása és az adóegység kimeneti teljesítménye maximum 1W lehet. Az ISM sávok szabad használata miatt, igyekezni kell az azonos sávban működő többi eszközzel kialakuló RF interferencia elkerülésére. (Geier [2005])

Ortogonális frekvenciaosztásos multiplexelés

Az ortogonális frekvenciaosztásos multiplexelés (OFDM, Orthogonal Frequency Division Multiplexing) az FSK-val, PSK-val vagy QAM-al átalakított jelet több adott csatornához tartozó részvivő között osztja el. Ez a módszer rendkívül hatékony és nagysebességű adatátvitel területén egyre népszerűbb, mert nagyobb átviteli sebességet lehet elérni vele a többutas terjedésből adódó problémák minimálisra csökkentésével (pl. az IEEE 802.11g szabvány része). Ezen kívül az OFDM-moduláció az utóbbi időben támogatja a nagysebességű telefonhálózatokhoz kifejlesztett ADSL szabvány alkalmazását is.

1.4. IEEE 802.11 fizikai rétegek

Az eredeti, 1997-ben elfogadott IEEE 802.11 szabvány frekvenciaugrásos szórt spektrumú (FHSS) és direkt sorozatú szórt spektrumú (DHSS) fizikai réteget tartalmaz, melyek a 2,4 GHz-es sávban maximum 2 Mb/s adatátviteli sebesség mellett működnek, ezért kevés cég kínál ezzel a technológiával terméket. Az FHSS szélessávú jelet továbbít, mely lefedi a teljes 2,4 GHz-es tartományt. Az FHSS nem működik együtt semmilyen más 802.11 fizikai réteggel. Az IEEE 802.11 DSSS fizikai réteg is legfeljebb 2 Mb/s adatátviteli sebességre képes. (Geier [2005]) A 802.11 szabványokat az 1. táblázat hasonlítja össze.

1. táblázat: IEEE 802.11 szabványok. Forrás: saját összeállítás

	IEEE 802.11a	**IEEE 802.11b**	**IEEE 802.11g**	**IEEE 802.11n**
Szabvány elfogadásának éve	1999	1999	2003	2009
Adatátviteli sebesség (elméleti)	54 Mbps (30m)	11Mbps (100m)	54 Mpbs (30-37m)	300 Mpbs (50m)
Effektív átviteli sebesség	20-23	4 Mbps	20 Mbps	90-100 Mbps
Működési frekvenciatartomány	5 GHz	2,4 GHz	2,4 GHz	2,4/5 GHz
Csatornák száma	12	14	14	14/12
Modulációs technika	OFDM	DSSS	OFDM, DSSS	MIMO-OFDM
Sávszélesség	20 MHz	20 MHz	20 MHz	20/40 MHz

Az **IEEE 802.11a** szabvány által használt 5 GHz-es tartomány előnyős, mert nem telített még, így nagyobb teljesítményszint elérése válik lehetővé a felhasználók számára. Ezen tartománynak viszont hátránya, hogy korlátozott a hatótávolság. Az 5 GHz használatából adódóan kisebb az interferencia lehetősége. A 802.11a szabvány nem kompatibilis a többi szabvánnyal. A 802.11a modulátorok különböző modulációs technikákat alkalmaznak: alacsonyabb átviteli sebességnél (6 Mb/s) BPSK modulációt (bináris PSK), míg nagyobb sebesség esetén (54 Mb/s) QAM modulációt alkalmaznak. (Geier [2005])

Az **IEEE 802.11b** szabvány egyik nagy előnye, hogy viszonylag nagy hatótávolsággal rendelkezik, így kevesebb hozzáférési pont szükséges a hálózatban. Hátránya, hogy a 2,4 GHz-es sávban összesen elérhető 14 csatornából 3 csatornát lehet használni (általában a 1, 6, 11 csatornákat használják) úgy, hogy ne legyen interferencia. Azonban emiatt a hálózat teljes kapacitása erősen csökken. Másik hátrány, hogy a szabvány más RF eszközökből származó

interferenciára érzékeny. Az IEEE 802.11b szabvány az adatkeretek jeleinek a 2,4 GHz-es frekvenciasáv 22 MHz-es részében történő szétterítésére DSSS-t használ. A modulátorok sebességfüggő modulációt alkalmaznak: kisebb sebességnél (1 Mb/s) különbségi bináris fázisbillentyűzést (Differential Binary Phase Shift Keying, DBPSK) használ, míg nagyobb sebességnél (2 Mb/s, 5,5 Mb/s, 11 Mb/s) különbségi kvadratúra-fázisbillentyűzést (Differential Quadrature Phase Shift Keying, DQPSK) használ. (Geier [2005])
Az IEEE 802.11g szabvány egyik nagy előnye, hogy lefelé kompatibilis. Azonban a 802.11b és 802.11g szabványok együttes használata során probléma merül fel, így különböző védelmi mechanizmusok alkalmazása szükséges, melyek korlátozzák a teljesítményt. A probléma forrása, hogy a két szabvány eltérő modulációs technikát használ, így a készülékek nem értik meg egymást. Ennek feloldására azonos modulációt kell használniuk, és így kell jelezniük egymás felé az átviteli közeg használatának szándékát. Az IEEE 802.11g szabvány is 3 nem átlapolódó csatornával rendelkezik, és érzékeny az RF interferenciára. (Geier [2005])

Az **IEEE 802.11n** szabványt úgy fogadták el, hogy a 2007 óta életben lévő Draft2 tervezet összes eleme belekerült a végleges szabványba, így biztosítva a kompatibilitás. A szabvány elsődleges célja az átviteli sebesség növelése volt. A 802.11n szabvány esetében a következő újításokkal érték el a megnövekedett sebességet[2]:

- Több segédvivőt használ: 48 db OFDM segédvivő helyett 52 db segédvivőt használ.
- Keretek közötti időt a felére csökkentette (800ns-ről 400ns-ra)
- MIMO: Míg a 802.11a/g szabvány 1 db adó- és 1 db vevő áramkörrel rendelkezik, addig a 802.11n szabvány által alkalmazott MIMO technológia lehetővé teszi maximum 4 db adó és 4 db vevő együttes alkalmazását.
- Csatornák összevonása: az előző szabványok esetében a csatornák 20 MHz sávszélességűek voltak, azonban a 802.11n megengedi a szomszédos csatornák összevonását, így 40 MHz-es csatornát használ kétszer annyi segédvivővel (108).
- Többletterhelés csökkentése: keretek egyesítése, maximális keretméret 4 KB-ról 64KB-ra növekedett, és az egyesített kereteket egyszerre nyugtázzák

[2] http://nik.bmf.hu/schubert.tamas/H%e1l%f3zati%20szolg%e1ltat%e1sok%20tervez%e9se%20%e9s%20m%fbk%f6dtet%e9se/WLAN%20MSc-2008.pdf

2. Irodai WLAN eszközei, azok funkciói

A 802.11 vezeték nélküli hálózatok népszerűségének növekedésével sok cég kezdett vezeték nélküli eszközök fejlesztésébe, gyártásába. A világ egyik legnagyobb hálózati termékeket gyártó cége a Cisco Systems Inc., mely a vezeték nélküli technológiában is élen jár. A Cisco 2000-ben megvásárolta az Aironet nevű céget, mely később névadója lett a Cisco vezeték nélküli termékcsaládnak. Ebben a fejezetben bemutatásra kerülnek a Cisco által forgalmazott, a vezeték nélküli hálózatok felépítő eszközök: hozzáférési pontok (AP), WLAN vezérlők (WLAN Controller), kliens adapterek (Client Adapter), és egyéb eszközök (vezeték nélküli forgalomirányítók és kapcsolók, vezeték nélküli IP-telefonok, vezeték nélküli hidak). (Velte-Velte [2005])

2.1. Vezeték nélküli eszközök

2.1.1. Cisco Aironet AP

A hozzáférési pontok olyan a LAN-hoz csatlakoztatott eszközök, melyek vezeték nélküli hozzáférést biztosítanak a hálózathoz. A vezeték nélküli kliensek a vezetékes vagy vezeték nélküli hálózat eléréséhez az AP-val kommunikálnak. Az AP lehet akár egy teljesen vezeték nélküli hálózat középpontja vagy lehet a csatlakozási pont a vezetékes és vezeték nélküli hálózat között. A következő tényezők fontosak a megfelelő AP kiválasztásához:

- a vezeték nélküli hálózatot használó eszközök száma,
- a kívánt sebesség és hatótávolság (milyen távolságban legyen használható a WLAN),
- a költségvetés.

Az Aironet 1130AG hozzáférési pont az optimális lefedettség érdekében kettő beépített rádióegységgel rendelkezik (802.11a/g támogatására) 1-1 antennával ellátva, melyek lehetővé teszik a körsugárzást. A két szabványt is támogató eszköz elvben akár 108 Mb/s adatátviteli sebességre is képes. Az 1130AG AP támogatja a 802.11i, a WPA (WiFi Protected Access), a WPA2, és az EAP számos típusának használatát a biztonságos hálózat kialakításhoz.

Az 1200-as szériába tartozó Cisco 1250 AP egy moduláris hozzáférési pont, melynek flexibilis konfigurálhatósága optimális megoldást kínál a vezeték nélküli kapcsolat kialakítására a 2,4 GHz-es és 5 GHz-es tartományban, a 802.11a/g/n szabványok

használatával. A Cisco Aironet 1250 esetében az új technológia alkalmazása mellet hangsúlyt fektettek a biztonságra is (802.11i, WPA és WPA2, 802.1X a hozzá kapcsolódó EAP típusokkal együtt: EAP-TLS, EAP- TTLS/MSCHAPv2, EAP-FAST, stb.). Az Aironet 1250 AP támogatja a PoE szabványt és a QoS használatát. Az 1230AG hozzáférési pont az előbb bemutatott hozzáférési pontoktól annyiban tér el, hogy ehhez a típushoz lehet külső antennát is csatlakoztatni. (Velte-Velte [2005])

2.1.2. Lightweight AP, WLAN Vezérlők

Az előzőekben bemutatott hozzáférési pontokat hagyományos (legacy) hozzáférési pontoknak nevezik és hagyományos vezeték nélküli megoldást nyújtanak. Az előbb említett Cisco 1130AG hozzáférési pont egyben **Lightweight Hozzáférési Pont** (LAP) is, mely támogatja a 802.11a/b/g szabványt, két sávon üzemel (dual band), konfigurációt és menedzselést nem igénylő hozzáférési pont, mely biztonságos úton, nagyvállalati környezetben költséghatékony vezeték nélküli hozzáférést biztosít a fejlett WLAN szolgáltatásokhoz. A Cisco 1130AG LAP a Cisco Wireless LAN Controller (WLC) támogatásával együtt működik. Az LAP és WLC mellett a hálózati monitorozás érdekében a hálózatban található még egy Cisco Wireless Controll System (WCS). Az Cisco 1130AG lehetővé teszi a PoE (Power over Ethernet) és a QoS használatát. Az LAP-t a WLC látja el utasításokkal és funkciói központosítva vannak. Az LAP információkkal láthatja el a WLC-t és a WCS-t, így azok valós idejű döntéseket hozhatnak. (Velte-Velte [2005])

A **Cisco WLC** (WLAN Controller), a WCS-sel és az Aironet hozzáférési pontokkal (LAP) együttműködve, lehetővé teszi a hálózati rendszergazdáknak, hogy biztonságosan menedzseljék a WLAN-okat és a mobilitás szolgáltatásokat (pl. hang, vendéghozzáférés). A WLC eszközön kerülnek tárolásra az LAP beállításai, és ezeket a WLC-től kapja meg (hang- és adatszolgáltatások, biztonsági szabályok, behatolásmegelőzés (intrusion prevention), RF menedzsment, QoS, LAP konfigurációk).

A WLC az LWAPP (Lightweight AP Protocol) használatával Layer2 és Layer3 infrastruktúrán keresztül kommunikál a hozzáférési pontokkal. A Cisco 2100 sorozatában három modellt kínál: Cisco 2125 WLC, Cisco 2112 WLC és Cisco 2106 WLC. Ezek a modellek eltérnek a támogatott LAP-k számában, a rendelkezésre álló portokban és egyéb szolgáltatásokban (pl. PoE). Így például a Cisco 2112 WLC legfeljebb 12 LAP vezérlését

támogatja, és 8 Ethernet interfésszel rendelkezik, melyből kettő PoE port. (Velte-Velte [2005])

A WLC érzékeli, és alkalmazkodik a rádiós környezet változásához (RF menedzsment), lehetővé téve a következő funkciók megvalósulását:

- csatornák dinamikus kiosztása, csökkentve az interferencia lehetőségét
- a rendszer érzékeli az interferenciát, és megváltoztatja a hálózat beállítását ezzel csökkentve az interferencia hatását
- terheléselosztást végez, így sok felhasználó esetén nem lesz egyetlen LAP sem túlterhelve
- a hozzáférési pontok teljesítményét szabályozva megfelelő, lefedetlen területet nem tartalmazó hálózatot tud létrehozni.

A WLC naprakész biztonsági beállításokat használ, pl. WPA2, WPA, különböző EAP típusok. A WLC további biztonsági szolgáltatásai közé tartozik a nem kívánt rádiós sugárzás érzékelése és elkerülése, behatolások megelőzése az idegen (rouge) AP blokkolásával és fizikai meghatározásával, kliensek házirend alapján való menedzselése a hálózati hozzáféréshez. (Velte-Velte [2005])

2.1.3. Hálózati interfészkártya (NIC, Client adapter)

A vezeték nélküli hálózat elengedhetetlen eleme a (vezeték nélküli) hálózati interfészkártya, mely a felhasználókat a vezeték nélküli hálózathoz csatlakoztatja. A Cisco Aironet termékcsaládban a következő hálózati kártyákat találhatjuk: Cisco Aironet 350, Cisco Aironet 802.11a/b/g CardBus és PCI Wireless Client LAN Adapter. A kártya kiválasztásánál a rendelkezésre álló kliens és a vezeték nélküli hálózat típusa a döntő tényező.

Cisco Aironet 802.11a/b/g CardBus és PCI Wireless Client LAN Adapterrel lehetővé válik számos alkalmazás használata. A PCI kártya ideális az asztali számítógépekbe, míg a CardBus kártyák a laptopoknál használhatók. A CardBus eszközöket a laptop megfelelő slotjába (aljzatába) kell behelyezni (esetleg egy CardBus/PCMCIA átalakító használatával). A PCI eszköz egy kártya, amit az alaplap PCI slotjába kell helyezni. A kártyához csatlakozik egy kis antenna, melyet állítani lehet a jobb minőségű adás-vételhez. Mind a két fajta vezeték nélküli kliens adapter támogatja a 802.11a/b/g szabványokat, a 802.11a és 802.11g szabványok (dual mode) és a 802.11a, 802.11b és 802.11g szabványok egyidejű használatát is

(trimode). Ezek az eszközök támogatják a WPA és WPA2, továbbá a 802.1x hitelesítést, ami tartalmazza a következőket: LEAP, EAP-TLS, PEAP-GTC, EAP-FAST és PEAP-MSCHAP V2. (Velte-Velte [2005])

2.1.4. Egyéb eszközök a vezeték nélküli hálózatokban

A vezeték nélküli hálózatokban a fentebb ismertetett eszközökön kívül egyéb eszközökkel találkozhatunk. A 802.11 szabvány nem definiálja a **vezeték nélküli hidat** (wireless bridge, WB), mely két, ugyanolyan vagy eltérő Adatkapcsolati rétegbeli protokollt használó hálózatot kapcsol össze. A WB elsődleges feladata kapcsolat kialakítása más hidakkal és kapcsolat nyújtása egy vagy több hálózat felé. A Cisco kínálatában az Aironet 1300-as szériájú hozzáférési pont egyben WB is, mely pont-pont vagy pont-multipont hídként szolgálhat.
A Cisco további termékeket kínál a robosztusabb, több szolgáltatást nyújtó vezeték nélküli hálózatok kiépítéséhez. Erre példa a Cisco 3200 sorozatú **vezeték nélküli és mobil forgalomirányító**, mely a mozgó járművekbe szerelhető, így biztosítva vezeték nélküli hozzáférést külső helyszínen. A vezeték nélküli hálózatok népszerű eszköze a **vezeték nélküli IP-telefon** (pl. Cisco 7920). Az ilyen telefonokhoz szükséges a Cisco rendszerű hálózatokban egy Unified Communication Manager. (Velte-Velte [2005])

2.2. Antennák

A Cisco számos antennatípust kínál, melyek mind különböző helyzetekben használhatóak, eltérő funkciókkal és hatótávolsággal. A következőkben a vezeték nélküli hálózatokban leggyakrabban használt antennatípusokat ismertetem. (Velte-Velte [2005])
Az antennák egyik, általános csoportosítási módja a következő:

- Körsugárzó (omnidirectional) antennák: 360 fokos sugárzási minta jellemzi, melyet akkor használnak, ha minden irányba szeretnének lefedettséget biztosítani. Sugárzási mintájuk leginkább egy lapított gömbre hasonlít.
- Irányított (directional) antennák: energiájukat egy irányba fókuszálják és minél nagyobb az erősítés (gain), annál kisebb a sugárzási szög és annál nagyobb a hatótávolság (egyre kisebb lefedettség-terület mellett). Főként kültéri antennák, de vannak beltéri változatai is. Fő típusai: Yagi, patch, parabola.

- Elhalkulásmentes (diversity) antennák[3]: az elektromágneses hullámok visszaverődése miatt az antenna nem csupán egyetlen jelet fog, hanem bizonyos késéssel a többi visszavert jelet is veszi, ami ronthatja a vétel minőségét. Kettő vagy több antenna segítségével csökkenthető a többutas torzítás.

Antennák technikai jellemzői

Az antennákat számos technikai jellemző különbözteti meg egymástól. Az antenna egyik fontos jellemzője az **iránykarakterisztikája**, mely megadja az antenna körüli térben, az antenna által létrehozott azonos teljesítménysűrűségű pontokat. A viszonyítási alap a csak elméletben létező, pontszerű izotróp antenna, amely „gömbsugárzó", vagyis a tér minden irányában azonos mértékben sugároz. „A valóságos antennák azonban anizotrop jellegűek, azaz a köréjük rajzolt gömbfelület különböző részein különböző térerősséget létesítenek. Az antenna **sugárzási karakterisztikája** mutatja meg, hogy az antenna milyen irányban mekkora intenzitással sugároz. A sugárzási karakterisztikát két egymásra merőleges (pl. vízszintes és függőleges) síkban adják meg; a karakterisztika az adott síkban egyenlő térerősségű pontokat összekötő görbe."[4]

Teljesítmény paraméterek

Az antennákra jellemző egyik teljesítményparaméter - mely meghatározza, hogy az antenna milyen térben sugároz - a **sugárzási minta** (radiation pattern). A sugárzási minta az antenna által kibocsátott elektromágneses hullámtér relatív térerősségének geometriai mintázata[5]. Az ideális (izotróp) antennánál ez egy gömb alakzat.
„A teljesítmény szintek igen széles nagyságrendi határok között fordulnak elő a gyakorlatban, ezért a Watt mértékegység megtartása mellett egy logaritmikus kifejezési módszert is használnak teljesítményszintek számokkal történő ábrázolására."[6] Az antennákra jellemző paraméter még a **nyereség** (gain), ami a főirányban kisugárzott teljesítménysűrűség és az

[3] http://www.volkswagen.hu/volkswagen_koeruel/innovacio/m_szaki_lexikon/diversity_antennen.html

[4] http://wiki.ham.hu/index.php/Iránykarakterisztika

[5] http://www.tscm.com/radiapat.pdf

[6] http://www.secron.hu/Rádiótechnika.html

azonos bemenő teljesítményű izotróp antenna teljesítménysűrűségének hányadosa[7]. A nyereséget dB mértékegységben adjuk meg; ha a nyerség pozitív előjelű, akkor a jel erősítéséről beszélünk, ha pedig negatív előjelű, akkor csillapításáról beszélünk. A nyereség azt fejezi ki, hogy az antenna mennyire fókuszálja a kisugárzott rádiófrekvenciás energiát. A nyereség mérésérére két fajta módszer létezik a viszonyítási ponttól függően: az egyik a dBi, míg a másik a dBd. A dBi jelentése dB izotróp, vagyis itt a viszonyítási alap egy úgynevezett "izotróp" antenna szabad térbe sugárzott teljesítménye. A dBd jelentése dB dipole, vagyis itt a viszonyítási alap a "dipole" antenna fősugárzási irányba sugárzott teljesítménye. A "dipól" (dipole) azaz kétpólusú antenna valóságosan létező antennatípus.[8]

„Az antenna **polarizációján** az antenna fizikai orientációját értjük a vízszintes és a függőleges síkhoz képest." (Geier [2005] 146. old.) Az antenna polarizáltsága megfelel az általa kisugárzott hullám elektromos térerősség vektorának polarizáltságának. A polarizáció típusai: lineáris (függőleges, vízszintes), körkörös (jobb-kéz, bal-kéz). Például a vezeték nélküli lokális hálózatokban leggyakrabban előforduló függőleges polarizáció akkor valósul meg amikor az antenna merőleges a Föld felszínére. Vízszintes polarizáció akkor jelentkezik, amikor az antenna párhuzamos a Föld felszínével. Az adó és a vevő antennának azonos polaritásúnak kell lenni a rádiófrekvenciás energia átvitelének maximális kihasználásához. Ha ez a feltétel nem teljesül, nem jön létre a kommunikáció. (Geier [2005])

A **nyílásszög** (beamwidth) az iránysugárzó antennák irányhatásának mérőszáma, mely lehetővé teszi az iránysugárzó antennák közötti összehasonlítást azon tulajdonságuk alapján, hogy mennyire képesek a beléjük táplált teljesítményt egy nyalábba gyűjteni és egy konkrét irányba kisugározni. A nyílásszöget irányított antennák esetében definiáljuk.[8]

Az antennák táplálásához használatos koaxiális kábelekkel kapcsolatos fogalom a "**hullámellenállás**", mely az antennákat tápláló vezetékekhez kapcsolódik. A Wi-Fi eszközöknél a koaxiális kábelek használata terjedt el, melynek hullámellenállása praktikus megközelítéssel az az Ohm érték, amellyel egyező terhelést kapcsolva a kábel végére, minimális veszteséggel jut el a rádiófrekvenciás teljesítmény a terheléshez.[8] A hullámellenállás a belső ér külső átmérőjének és az azt körülfogó cső-alakú vezető belső átmérőjének arányától függ. A Wi-Fi hálózatokban 50 Ohm hullámellenállású koaxiális kábeleket használnak. A Wi-Fi rádióegységek és antennák ehhez illeszkednek.

---

[7] http://alpha.tmit.bme.hu/pub/jegyzet/radio.kom/new/anthull4.doc

[8] http://www.secron.hu/Rádiótechnika.html

2.3. Cisco Wireless Control System

A vezeték nélküli hálózatok általánosan ismert eszközei mellett egy korszerű, nagyvállalati rendszernek része egy dedikált menedzsmentrendszer is. Ilyen megoldást kínál a Cisco a Wireless Control System menedzsment platformjával.

Egy hatékony hálózatmenedzsment a hálózati leállások minimalizálásával sok pénzt takaríthat meg egy vállalatnak (pl. egy DoS támadás elkerülésével). „A vezeték nélküli hálózatok magas színvonalú üzemeltetése több területet foglal magában:

- a WLAN tervezése és kiépítése
- a hálózat monitorozása és teljesítményének optimalizálása
- a hálózat adatbiztonságának folyamatos fenntartása
- a WLAN hálózatban működő eszközök felügyelete és menedzsmentje”[9]

A Cisco által jelenleg nyújtott Cisco Unified Wireless Networking (Cisco Egységes Vezeték nélküli Hálózat) lehetővé teszi a vékony hozzáférési pontok (Lightweight AP) vezérlőn (controller) keresztüli menedzselését. A menedzsment e központosított formájának köszönhetően lehetővé válik, hogy a hozzáférési pontokon konzisztens biztonsági házirend legyen. Azonban a vállalat növekedésével több vezérlőre van szükség, és a menedzsment ellátásához már szükséges a WCS[10] (Wireless Control System, Vezeték nélküli Irányító Rendszer) használata. „A WCS egy böngésző alapú szoftver, melynek használatával lehetőség nyílik egy interfészen keresztül több irányító vezérlésére”. (Carroll [2009] 358. old.) A WCS számos szolgáltatása és opciója közül most kettőt mutatnék be: a hálózati térképeket és az aktív hálózati monitorozást.

Hálózati térképek a WCS-ben

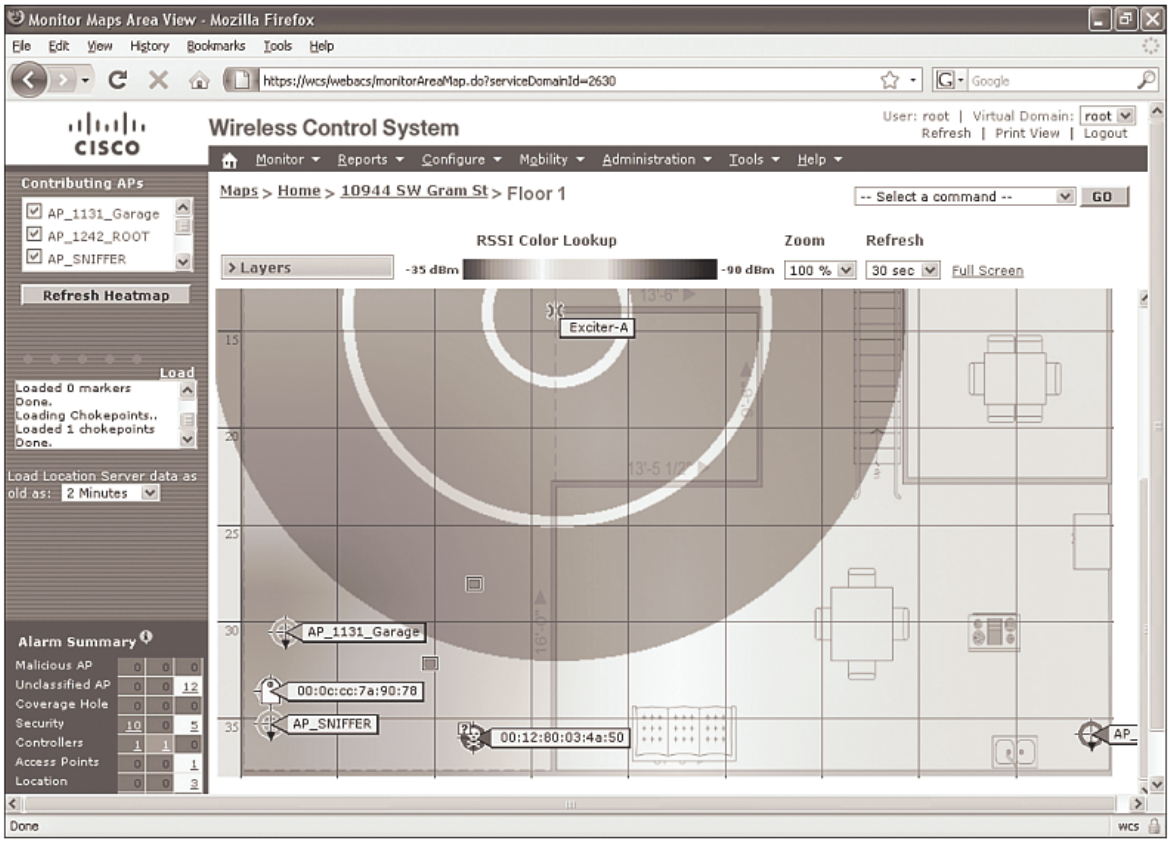
A WCS-ben található hálózati térképeket a vezeték nélküli hálózatok vizuális reprezentálására tervezték, és nem csak a kivitelezést követő monitorozásban, hanem az implementálási folyamatban is nagy segítséget nyújtanak. A WCS hálózati térképek használatával a menedzselt hálózatot valósághű térképeken lehet nézni.[11] Tervezői mód használatával

[9] http://www.bcs.hu/letoltes.php?d_id=823

[10] http://www.cisco.com/en/US/products/ps6305/products_data_sheets_list.html

[11] http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcsmaps.pdf

meghatározható a szükséges hozzáférési pontok száma, azok helye. A hálózati térképeket a Monitor > Maps menüpontból lehet elérni. Elsőnek egy épületet kell definiálni, majd azon belül egy szintet. Ha ezek megvannak, akkor hozzá lehet adni a hozzáférési pontokat. Az épület definiálása előtt azonban egy ún. campust kell létrehoznunk. A campuson belül, ha definiáltuk az épületet, megadhatjuk az épület adatait: az épület nevét, kapcsolattartó adatait, szintek számát, horizontális ill. vertikális dimenziók (lábban mért) értékét. A legördülő menüből hozzáadhatunk egy szintet, mely tulajdonképpen egy környezeti nézetet ad, melyben fontos adatokat határozhatunk meg: az emelet típusa, magassága, stb. (Carroll [2009])



2. ábra: Hőtérkép a WCS rendszerben

Forrás: http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsmaps.html#wp1077224

Az épület és szintek létrehozása után elkezdhetjük hozzáadni a hozzáférési pontokat. Az AP-k hozzáadásakor ügyelni kell a megfelelő antenna, AP típus, elhelyezés, konfiguráció megadására. Az AP elhelyezése után a WCS megbecsüli egy ún. hőtérképen (2. ábra), hogy az AP beállításával mekkora területen lehet fogni a jelet. A pontosabb becsülés érdekében különböző akadályokat lehet a térképen felvenni, mint pl. ablakok, ajtók, falak. A hőtérkép elsődleges célja a lefedettség demonstrálása. A WCS-ben található hőtérkép által megadott

jóslás azonban nem egyezik meg a vezeték nélküli hálózatok telepítésekor végzendő felméréssel (site survey). Ezen felmérések mindig mért adatok alapján készülnek, és egy aktuális állapotot tükröznek, míg a WCS-ben számított értékek alapján létrehozott térképet kapunk, amely azt határozhatja meg, hogy milyennek fog kinézni a hálózat. (Carroll [2009])

Hálózatmonitorozás a WCS használatával

A WCS lehetővé teszi a vezeték nélküli hálózat valós idejű monitorozását (megfigyelését). A Monitor fülre kattintva számos eszközt monitorozhatunk: vezérlőket, hozzáférési pontokat és egyéb eszközöket.

A WCS egy riasztási összefoglalót (Alarm Summary) nyújt, mely minden 15 percben frissül: ahol nincs jelzés, ott minden rendben van; a vörös színű területek kritikus riasztásra utalnak, míg a narancssárga és sárga területek súlyos és kevésbé súlyos riasztást mutatnak. A riasztásra kattintva megtekinthető az adott helyzetről található részletes jelentés.

A WCS másik fontos eleme a kliens eszközök hibaelhárítása, mely a Monitor > Client menüpontból érhető el. A menüpontba lépve a Client MacAddress (Kliens MAC-cím) mezőbe beírhatjuk a kliens MAC-címét és a Troubleshoot (Hibaelhárítás) gombra kattintva lehetőség nyílik az adott kliensen hibaelhárítási feladatokat végezni.

A WCS-ben továbbá lehetőség van az idegen hozzáférési pontok, biztonsági beállítások és a Radio Resource Management (Rádiós Erőforrás Menedzsment) monitorozására. A WCS által támogatott Location Appliances (helyzet meghatározó alkalmazások) segítségével valós idejű nyomkövetést lehet végrehajtani, és akár 5-10 méteres pontossággal meg lehet határozni az eszköz helyzetét. Ez különösen RF interferencia esetén és idegen eszköz felderítésénél hasznos. (Carroll [2009])

3. WLAN hitelesítés RADIUS használatával

A 802.1x szabvány használatával (mely a 4. fejezetben kerül ismertetésre) jelentősen biztonságosabb vezeték nélküli hálózatot lehet kiépíteni. A 802.1x szabvány által opcionálisan megjelölt RADIUS protokollnak nagy szerepe van az osztott kulcsú hitelesítés biztonságos implementációjában. A következőkben röviden bemutatásra kerül a RADIUS működése és a hozzá tartozó infrastruktúra.

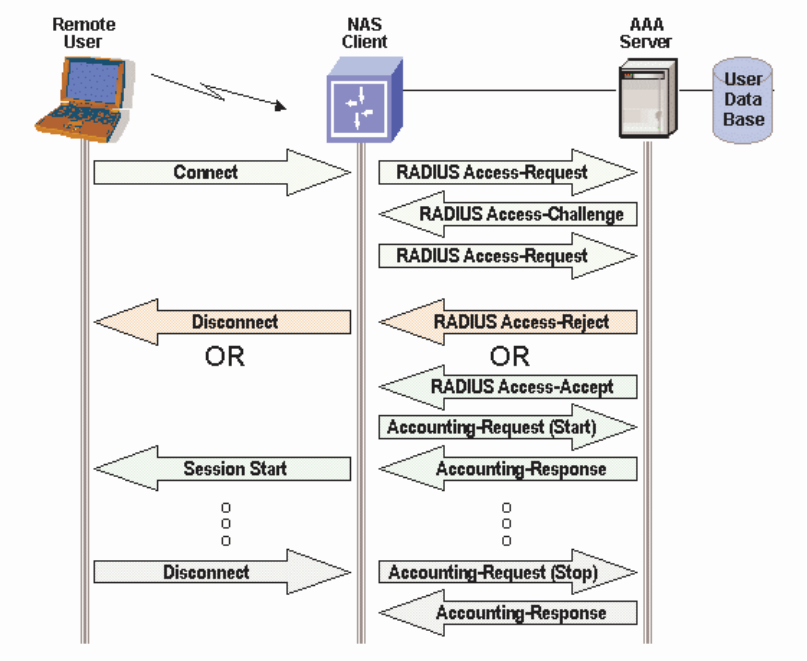
3.1. AAA megvalósítása RADIUS protokollal[12]

A Remote Authentication Dial In User Service (RADIUS – távoli hitelesítő, betárcsázós felhasználói szolgáltatás) protokollt eredetileg AAA (Authentication, Authorization, and Accounting – Hitelesítés, Hozzáférés, Naplózás) célokra hozták létre a SLIP és PPP betárcsázós kapcsolatok központosított hitelesítéséhez. A RADIUS az RFC 2865 dokumentumban van definiálva. Nagyszámú felhasználó mellett megnövekedik az adminisztrációs munka. Az AAA-t legjobban egy egyedi adatbázis fenntartásával lehet megvalósítani, mely felhasználókat tartalmaz, mely alapján biztosítható a hitelesítés és jogokat lehet biztosítani.[13] A RADIUS az *Access-Request* üzeneteket (hozzáférési kérelmek) egy hitelesítő szervernek (AS) továbbítja így lehetővé válik, hogy ne kelljen fenntartani minden hálózati hozzáférést vezérlő szervernél (Network Access Server – NAS, de gyakran AAA szervernek is mondják) egy listát a felhasználói nevekről és jelszavakról (3. ábra).
Amikor egy felhasználó csatlakozni kíván a hálózathoz, a NAS egy *Access-Request* üzenetet küld az AAA szervernek, melyben a kapcsolat adatai találhatóak: a felhasználói név, a kapcsolat típusa (melyik porton kapcsolódott), a NAS identitás és a Hitelesítő (Authenticator). Az AAA szerver miután fogadta a kérelmet a csomag forrása, a NAS identitása és a Hitelesítő alapján meghatározza, hogy a NAS jogosult-e ilyen kérelem küldésére. Ha igen, akkor a szerver megkeresi a felhasználói nevet és a jelszót az adatbázisban, és esetleg más – az *Access-Request* üzenetben található – attribútumok alapján meghozza az engedélyezési döntést. A használt hitelesítési metódustól függően az AAA szerver válaszolhat egy véletlen számot tartalmazó *Access-Challange* üzenettel, melyet a NAS továbbít a távoli felhasználó

[12] http://www.wi-fiplanet.com/tutorials/article.php/3114511

[13] ftp://ftp.rfc-editor.org/in-notes/rfc2865.txt

felé (pl. CHAP használatával), akinek a megfelelő értékkel kell válaszolnia (pl. a saját jelszavával titkosítja a kihívást). Az üzenetet ezután a NAS továbbítja az AAA szervernek egy *Access-Request* üzenet formájában. Az AAA szerver a döntés alapján vagy fogadja a csatlakozási kérelmet (*Access-Accept* üzenet visszaküldése), vagy elutasítja (*Access-Reject* üzenet visszaküldése). A felhasználó hitelesítése lezárul az Access-Accept üzenet küldése után, és megkapja a hozzáférést a kért szolgáltatásokhoz. Sikertelen csatlakozási kísérlet esetén a NAS bontja a kapcsolatot a felhasználóval. Ha az Accounting engedélyezve van és a NAS egy Access-Accept üzenetet kap, akkor a NAS egy *Accounting-Request (Start)* üzenetet küld az AAA szervernek, ami egy rekordot hoz létre és nyugtázza a kérelmet, míg a NAS aktívvá teszi a felhasználói kapcsolatát. A kapcsolat végén egy *Accounting-Request (Stop)* üzenettel jelzi a NAS, hogy mennyi ideig tartott a kapcsolat és mi volt a kapcsolat megszakadásának az oka.



3. ábra: A RADIUS architektúra felépítése

Forrás: http://www.wi-fiplanet.com/img/tutorial-radius-fig1.gif

3.2. Biztonság és kiterjeszthetőség[14]

A RADIUS üzenetek UDP protokollon keresztül kerülnek szállításra és a következő mezőket tartalmazzák: üzenet típusa, hossz, Hitelesítő (Authenticator) és Attribútum-Érték párokat

[14] http://www.wi-fiplanet.com/tutorials/article.php/3114511

(Attribute-Value pair, AV)[15]. A NAS és az AAA szerver a Hitelesítőt használják arra, hogy megbizonyosodjanak arról, hogy mind a ketten ismerik a titkos jelszót, illetve a Hitelesítő figyeli a RADIUS válaszok eredetiségét. A Hitelesítőt a felhasználó jelszavának elfedésére használják arra az esetre, ha valaki lehallgatná a RADIUS üzeneteket. Az *Access-Request* üzenetben elküldött Hitelesítő mező egy véletlen számot tartalmaz, melynek MD5 kivonatát XOR-olják a felhasználó jelszavával és az *Access-Request* üzenet User-Password attribútuma fogja tartalmazni. Ezután minden RADIUS üzenet tartalmaz egy MD5 kivonatot a titkos jelszóról, a Hitelesítőről és egyéb, a válaszban található értékről.

A Hitelesítő meggátolja a passzív lehallgatás, de ha a támadó mind az *Access-Request*, mind az *Access-Response* csomagokat elfogja, akkor egy szótártámadást hajthat végre a titkos jelszó meghatározásához. Ezért ajánlatos hosszú és véletlen jelszót használni, és (amennyiben lehetséges) biztonságos médiumot. Az ismert sebezhető pontokról és a kockázatok minimalizálásáról az RFC 3580 dokumentum tájékoztat.

A RADIUS által szállított információk AV párokban vannak reprezentálva, melyek flexibilitást nyújtanak. Az eredeti szabványban definiált AV párok mellett (pl. User-Name, User-Password, stb.) a gyártók definiálhatnak új AV párokat saját, gyártó specifikus adatok szállítására. (Pl. az RFC2548 dokumentumban a Microsoft definiált az MS-CHAP protokollhoz AV párokat.)

3.3. RADIUS használata WLAN-okban[16]

A 802.1x Port Access Control-t (port hozzáférés vezérlés) használó vezeték nélküli hálózatokban a vezeték nélküli állomás a távoli felhasználó és a vezeték nélküli AP pedig a NAS. A vezeték nélküli állomások a 802.11 protokollok segítségével asszociálnak a hozzáférési ponthoz, nem pedig valamilyen betárcsázós protokollon keresztül (pl. PPP). Az állomások asszociálás után, rögtön egy *EAP-Start* üzenetet küldenek az AP-nak, ami ezt követően kéri az állomás adatait azonosítás céljából, majd továbbítja azokat az AAA szervernek egy *Access-Request* csomagban. Az AAA szerver és az állomás a hitelesítést az AP-n keresztül áthaladó *Access-Challange* és *Access-Request* üzenetek feldolgozásával végzi. A feldolgozás történhet titkos csatornán az EAP típusától függően. Amint az AAA szerver

[15] http://technet.microsoft.com/hu-hu/library/cc726017(WS.10).aspx

[16] http://www.wi-fiplanet.com/tutorials/article.php/3114511

elküldi az *Access-Accept üzenetet* az AP és az állomás befejezi a kapcsolat kiépítését és legenerálják a session kulcsokat a WEP vagy TKIP segítségével. Ezen a ponton az AP engedélyezi a portot és az állomás jogosulttá válik adatok küldésére és fogadására. *Access-Reject* üzenet érkezése esetén az AP bontja a kapcsolatot az állomással. Az állomás az újból megpróbálhatja a csatlakozást és hitelesítést, de amíg a hitelesítés nem sikeres, nem tud adatot küldeni az AP-n keresztül a hálózatba. A RADIUS üzenetekben lévő AV párok segítségével az AAA szerver közli a hozzáférési ponttal és az állomással a kapcsolatra vonatkozó paramétereket, pl. Session-Timeout vagy VLAN címke.

3.4. Implementációs lehetőségek[17]

Amennyiben 802.1x keretrendszert használva szeretnénk hitelesíteni a hálózatba csatlakozó felhasználókat, akkor számos opció közül választhatunk. Ha már rendelkezünk egy AAA szerverrel, ami a RADIUS protokollt is támogatja, akkor ki kell választani a megfelelő EAP típust, majd konfigurálni a szervert és klienseket. Ha olyan AAA szerverünk van, mely támogatja a RADIUS-t, de a 802.1x szabványt nem, akkor frissíthetjük a szerverünket, vagy új szervert is üzembe helyezhetünk. Ha utóbbi mellett döntünk, akkor számos tényezőt figyelembe kell venni: meglévő infrastruktúra, rendelkezésre álló költségvetés, stb.
Meglévő Microsoft Windows Serverrel ellátott hálózatban telepíthetjük a Microsoft RADIUS szerverét, amennyiben valamelyik szerveren van erre kapacitás. Ehhez az ISA (Internet Authentication Server) program- és szolgáltatáscsomagot kell telepíteni a Windows Serveren. A Microsoft alapú hitelesítés esetében célszerű, ha a vállalat rendelkezik megfelelő támogató személyzettel és a WLAN-t használó állomásokon Windows operációs rendszer fut. Amennyiben az előbbiekben említett feltételek nem adottak, lehetőség van valamilyen ingyenes, nyílt forráskódú RADIUS szerver telepítésére (pl. FreeRADIUS). Ha az eddig ismertetett megoldások egyike sem kivitelezhető, akkor a piacon különböző szolgáltatók nyújtanak RADIUS szolgáltatást. A vállalat szerződést köt a szolgáltatóval, amely biztosítja a felhasználók hitelesítését. Ilyen szolgáltatást nyújt többek közt az Aradial WiFi, Infoblox RADIUS One Appliance és még sokan mások a piacon.[18]

---

[17] http://www.wi-fiplanet.com/tutorials/article.php/10724_3114511_2

[18] http://www.wi-fiplanet.com/tutorials/article.php/3287481

4. Hitelesítési és titkosítási módszerek ismertetése

4.1. WLAN hitelesítési módszerek

A 802.11 szabvány hitelesítési keretrendszere a 802.11 hitelesítési menedzsment-keretet foglalja magában, mely megkönnyíti a nyílt és osztott kulcsú hitelesítés használatát, de önmagában a keretrendszer nem hitelesíti a klienst. Roshan és Leary (Roshan–Leary [2003] 132. old.) a következő komponensek hiányát nevezte meg a 802.11 szabványban, melyek hiányoznak a hatékony hitelesítéshez:

- központosított, felhasználó-alapú hitelesítés
- dinamikus hitelesítési kulcsok
- hitelesítési kulcs-menedzsment
- kölcsönös hitelesítés

A felhasználó-alapú hitelesítés elengedhetetlen, mert az eszköz-alapú hitelesítés (nyílt és osztott kulcsú hitelesítés) nem akadályozza meg a nem hitelesített felhasználókat a hitelesített eszközök használatától. A központosított felhasználó-alapú hitelesítés esetén AAA szerverek használatával (pl. RADIUS) lehetőség nyílik az eszközök és szolgáltatások biztosítására/megtagadására adott felhasználóknak függetlenül attól, hogy milyen eszközt használnak. A felhasználó-alapú hitelesítés másik előnye, hogy a felhasználóknak egyedi titkosítási kulcsuk van, így a dinamikus titkosítási kulcsok létrehozását támogató hitelesítési módszerek kiválóan beleillenek a WLAN biztonsági és menedzsment modellbe. A kulcsok automatikusan generálódnak a felhasználó hitelesítésekor, és érvénytelenné válnak, amikor a felhasználó lecsatlakozik a hálózatról, így a rendszergazdának nem kell statikusan kezelni a kulcsokat. A kölcsönös hitelesítés egy kétirányú hitelesítési folyamat, mely során nem csak a hálózat hitelesíti a klienst, hanem a kliens is hitelesíti a hálózatot. A nyílt és osztott kulcsú hitelesítés során az AP vagy a hálózat hitelesíti a klienst, de a kliens nem lehet biztos abban, hogy az őt hitelesítő AP egy valós eszköz (azaz nem idegen AP), mivel nincs erre megfelelő mechanizmus a 802.11 szabványban. A 802.11 gyártók és az IEEE felmérte a meglévő hitelesítési és titkosítási módszerek hibáit és ezek egy részét a 802.11i szabványban, míg más részét a 802.1x hitelesítési keretrendszerben orvosolta. A 802.1x keretrendszerről későbbiekben lesz részletesebben szó. (Roshan–Leary [2003])

4.1.1. Nyílt hitelesítés

A nyílt hitelesítés egy egyszerű üzenetcsere, mely során egy kezdeményező fél (rendszerint WLAN kliens, laptop vagy PDA) üzenet küld a hozzáférési pontnak, ami feldolgozás után a egy válaszüzenetben közli a hitelesítés állapotát (sikeres, sikertelen). A nyílt hitelesítést null-hitelesítésnek is nevezik, mert bármilyen kliens hitelesítését lehetővé teszi és nem nyújt semmilyen biztonságot (alapértelmezetten minden eszközben megbízik). Egyetlen „biztonsági" kritérium, hogy az eszköznek ismernie kell az AP által hirdetett SSID-t. A hálózatban lehet MAC-cím alapú hitelesítés is, azonban ez sem túl. A nyílt hitelesítés nem támaszkodik és nem is veszi igénybe az AAA szolgáltatásokat, így nincs szükség AAA infrastruktúrára. Ez a hitelesítési forma megfelelően alkalmazható nyilvános helyeken, mint például repülőtereken, kávéházakban, hotelekben, konferencia termekben. Ha a felhasználók egy nyílt hitelesítést alkalmazó hálózathoz csatlakoznak, akkor egyénileg kell gondoskodniuk a védelemről (szoftveres vagy hardveres tűzfallal). (Sankar–Sundaralingam–Miller–Balinsky [2004])

4.1.2. MAC alapú hitelesítés

A MAC-alapú hitelesítés (vagy MAC-címszűrés) az AP által felállított belső házirend, melyben azok a MAC-címek vannak tárolva, amelyeknek engedélyezett a csatlakozás. A címekről az AP táblázatot tart fent. Mivel a MAC-alapú hitelesítés nem része a 802.11 szabványnak ezért az implementálása különböző eszközökben eltérhet. A MAC-alapú hitelesítést végző eszköz megbízik a regisztrált MAC-cím integritásában (az eszköz feltételezi, hogy az adott MAC-cím ahhoz az eszközhöz tartozik) illetve a fogadó megbízik a küldött üzenetben, mivel az üzenet integritása sincs garantálva. A MAC-alapú hitelesítés semmilyen AAA szolgáltatást nem vesz igénybe, ezért a MAC-címeket manuálisan kell felvenni (minden hozzáférési pontnál egyenként) az AP MAC-cím táblájába. Ez a művelet sok adminisztratív munkával jár, és kevéssé növeli a biztonságot. A MAC-alapú hitelesítés megfelelő lehet kevés állomással rendelkező otthoni és kisebb irodai hálózatok esetében, de csak, mint kiegészítés a megfelelő védelem mellett. A MAC-címek meghatározása könnyű, mert a hálózati forgalom figyelésével a támadó egyszerűen kiolvashatja a keretekben látható – titkosítatlan – MAC-címeket és használhatja azokat. A nyílt hitelesítés minden hátránya igaz a MAC-alapú hitelesítésre is. A biztonságos kapcsolat érdekében VPN használata javasolt, míg

az Interneten böngésző felhasználónak pedig tűzfalat kell használniuk (szoftveres vagy hardveres). (Sankar et al. [2004])

4.1.3. Osztott kulcsú hitelesítés

A vezeték nélküli helyi hálózatok világában az osztott kulcsos hitelesítés biztonságosnak számít, melynek alapja a kihívás-válasz (challenge-response) protokoll. Az osztott kulcsú hitelesítés 6 lépésből áll, mely során 4 üzenetváltásra kerül sor (ún. 4 utas kézfogás):

1. a kezdeményező fél egy hitelesítési kérelmet küld a hozzáférési pontnak
2. az AP egy kihívással válaszol erre a kérelemre
3. a kérelmező titkosítja a kihívási szöveget a kulcsával
4. a kérelmező a titkosított üzenetet visszaküldi a hozzáférési pontnak
5. a hozzáférési pont dekódolja a szöveget
6. a dekódolt szöveg és egyéb feltételek teljesülésének vizsgálata, majd ennek tükrében a megfelelő lépések megtétele (pl. engedélyezés/megtagadás)

Az osztott kulcsú hitelesítés a titkosítási protokollt (pl. WEP) támogató és a kulcsok sávon kívüli (out-of-band) szállításához szükséges infrastruktúrát igényel. A kulcsot manuálisan kell megadni a csatlakoztatni kívánt eszközön és a hozzáférési ponton is. Az osztott kulcsú hitelesítésnél a fő probléma a sávon kívüli, manuális kulcskiosztás minden eszköz számára, illetve az, hogy eszközöket hitelesít és nem felhasználókat. A WEP például szimmetrikus titkosítást használ, ezért az entitások közötti kulcshozzárendelés (eszköz-kulcs pár) nem skálázható. Az osztott kulcsú hitelesítésnek jól dokumentált sebezhetőségei vannak. Számos Cisco AP a konfigurációja során nem ajánlja az osztott kulcsú hitelesítés használatát. (Sankar et al. [2004])

4.2. EAP Hitelesítési protokollok a WLAN-okban

4.2.1. Hozzáférés-vezérlési és hitelesítési mechanizmusok

„A hozzáférés engedélyezésének általános mechanizmusa, hogy mielőtt hozzáférési engedélyt adnánk az entitásnak (eszköz és/vagy felhasználó) hitelesítjük azt, valamilyen azonosító alapján.” (Sankar et al. [2004] 157. old) A hozzáférés-vezérlés kétállapotú: engedélyezzük

vagy megtagadjuk a hozzáférést valamilyen kritérium alapján. A hitelesítés egy három résztvevőből álló modell, melyben megtalálható: a *kérvényező (supplicant)*, aki a hozzáférést kérvényezi; a *hitelesítő (authenticator)*, aki a hozzáférést biztosítja; és a *hitelesítő szerver (authentication server)*, mely a jogokat adja. (Roshan-Leary [2003]) A kérvényezőnek van személyazonossága és néhány adata, mellyel bizonyítani tudja, hogy az, akinek állítja magát és a hálózathoz a hitelesítő egy szabályozott portján keresztül csatlakozik. A port koncepció nagyon fontos, mivel a hálózatban a kérvényező szempontjából ez lehet a szűk keresztmetszet a hálózati erőforrásokhoz való hozzáféréskor. Ezen port által egy ponton szabályozható a hálózat hozzáférése. Vezeték nélküli környezetben leggyakoribb kérvényező az állomás (laptop vagy PDA), és a hitelesítő pedig az AP. Egy állomás, egy időben egyszerre csak egy hozzáférési ponton keresztül csatlakozhat a hálózathoz. A hitelesítő önmagában nem tudja, hogy egy adott entitásnak biztosíthatja-e a hozzáférést, ezért van szükség a hitelesítő szerverre. A hitelesítőt az IETF hálózat-hozzáférési szervernek (Network Access Server, NAS) vagy RADIUS kliensnek nevezi. Számos esetben a hitelesítő és a hitelesítő szerver feladatát egy eszköz látja el, pl. egy 802.11 AP. A hitelesítés és hozzáférési jogok szabályozása általánosan a következőképpen néz ki: a kérvényező küld egy kérelmet a hálózati hozzáféréshez, majd EAP üzenetváltásra kerül sor a hitelesítővel. Bizonyos csomagváltások után a hitelesítő és a hitelesítő szerver közötti kommunikáció során eldől a hitelesítési protokoll. Ezután a kérvényező, hitelesítő és hitelesítő szerver közötti megfelelő információk cseréje következik, mely a végén a kérvényező vagy megkapja a jogot a hitelesítőtől, vagy az megtagadja a hozzáférést.[19] A rétegelt hitelesítési modellben a rétegnek meghatározott feladataik vannak, melyekhez adott protokollok tartoznak. A legalsó rétegben a hozzáférési közeg található, ami bármilyen 802-es szabvány lehet: Ethernet, Token Ring, WLAN, stb. Az EAP specifikációk egy keretrendszert biztosítanak a hitelesítési információk cseréjéhez, az egyel fentebbi rétegben. A cseréhez nem szükséges az IP protokoll, hanem a szállítási rétegbeli protokoll feladata ezt megoldani. A 802.1x tulajdonképpen ezt a feladatot látja el. Az EAP nagyon flexibilis, így pl. az aktuális hitelesítési protokoll határozza meg, hogy milyen hitelesítési információk szükségesek és ezek hogyan cserélődnek. (Sankar et al. [2004])

[19] http://www.rfc-archive.org/getrfc.php?rfc=3748

4.2.2. EAP

Az EAP (Extensible Authentication Protocol – bővíthető hitelesítési protokoll) az RFC 2284 dokumentumban definiált flexibilis protokoll, mely tetszőleges hitelesítési információkat szállíthat. Az EAP nem teljes hitelesítési módszer, hanem hitelesítésre optimalizált szállító protokoll, mely keretet nyújt többféle hitelesítési eljáráshoz. Az EAP közvetlenül az adatkapcsolati rétegben működik, IP protokoll használata nélkül." (Orosz–Sztrik–Soong [2005] 2. old.) Az EAP protokollnak két nagy előnye van: elkülöníti az üzenetcserét a hitelesítés menetétől egy független réteg használatával; a független réteg használata ortogonális kiterjeszthetőséget eredményez, ami azt jelenti, hogy a hitelesítési folyamat funkcióját ki lehet terjeszteni egy újabb mechanizmus alkalmazásával anélkül, hogy az érintett EAP rétegben változást idéznénk elő. A 802.1x keretszabvány EAP-ot használ hitelesítésre, ezért többféle összetett hitelesítési séma alkalmazható, mint például Smart-kártya, Kerberos, nyilvános kulcs, egyszeri jelszó (OTP), stb. (Sankar et al. [2004]) A mellékletben található 1. táblázat összefoglalja a leggyakoribb hitelesítési eljárásokat.

4.2.3. 802.1x áttekintés

Az IEEE által kifejlesztett 802.1x szabvány egy port-alapú hitelesítést biztosít, melynek szereplői a kérvényező, a hitelesítő és a hitelesítő szerver. A 802.1x szabvány feladata az EAP csomagok küldése vezetékes vagy vezeték nélküli hálózatokban. A 802.1x használatával a hitelesítő csomagokat Ethernet vagy 802.11 keretekbe helyezzük. A 802.1x szabvány csak egy keretet nyújt, de nem határozza meg az információkat (szükséges személyi adatok és egyéb kihívás-válasz módszerek) vagy a hitelesítés módszerét (pl. hogyan történjen a hitelesítés, milyen információ alapján hitelesítünk és a döntések milyen módon születnek, stb.)[20]. A 802.1x szabvány fő koncepciója az, hogy a hálózathoz való hozzáférés egy ponton, egy porton keresztül történjen. Amikor egy vezeték nélküli csomópont hozzáférést kér a hálózati erőforrásokhoz, a hitelesítő azonosítást kér tőle. A vezeték nélküli kliens számára hitelesítés előtt kizárólag EAP üzenetek (EAPoL vagy EAPoWL) forgalmazása engedélyezett. Miután a kliens elküldte az azonosító üzenetet, megkezdődik a hitelesítési folyamat, melyben a kérvényező és a hitelesítő egymás között EAPoWL (EAP over WLAN)

[20] http://www.networkworld.com/research/2002/0506whatisit.html

protokollal kommunikál. A hitelesítő – melynek csak a kérvényező és hitelesítő szerver közötti üzenettovábbítás a feladata – átcsomagolja az EAP üzenetet RADIUS formátumra, majd továbbítja a hitelesítő szervernek. A hitelesítési folyamat végeztével, a hitelesítő szerver üzenetet küld a hitelesítőnek a hitelesítés eredményéről, melynek sikeressége esetén a hitelesítő megnyitja az adott portot a kérvényező számára. (Sankar et al. [2004])

4.3. WLAN titkosítási és adatintegritási protokollok

Az eredeti 802.11 szabvány néhány igen súlyos hiányt mutatott a biztonság terén, főleg a WEP biztonságához kötődően. A WEP feltörését követően (2001) a Wi-Fi Szövetség tagjainak szükségük volt a vezeték nélküli hálózatok biztonságos használatának biztosítására. Az IEEE 802.11i munkacsoportja megkezdte a (lassú) munkát, míg a Cisco az ügyfelei számára gyorsan kifejlesztett egy megoldást, mely egy jól definiált részét képezte a később elfogadott 802.11i szabványnak. A megoldást WPA (Wi-Fi Protected Access – Wi-Fi Védett Hozzáférés) névre keresztelték. A WPA – mely 2003-ban(!) jelent meg – egy olyan biztonsági csomag amely a régi hardverek számára fokozott biztonsági szolgáltatásokat nyújt. A nagyobb biztonságot kínáló 802.11i szabványt 2004-ben fogadták el, WPA2 néven. A 802.11i új titkosítási és adatintegritási algoritmusokat foglalt magába, melyek egy része együttműködött a hagyományos, WEP-et támogató eszközökkel, azonban az újabb AES (Advanced Encryption Standard) algoritmust használó eszközök esetében szükséges volt a hardvereszközök fejlesztésére. (Sankar et al. [2004])

4.3.1. IEEE 802.11i

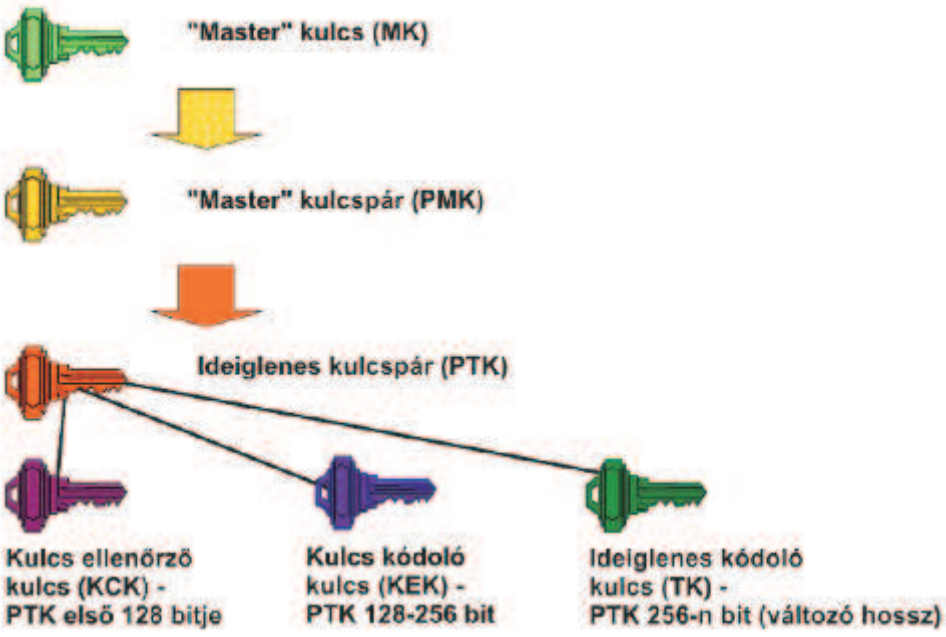
A 802.11i szabvány számos új biztonsági mechanizmussal biztosítja az üzenetek sértetlenségét és megbízhatóságát. Ezen mechanizmusok közül néhány csak kiegészítés ez előzőekhez, míg vannak teljesen új eljárások is. A 802.11i együttműködik a 802.1x szabvánnyal, így biztosítva egy keretet a kölcsönös hitelesítéshez és kulcsmenedzsmenthez[21].
A 802.11i újításai a következők voltak (Sankar et al. [2004] 141. old.):

[21] http://www.wi-fiplanet.com/news/article.php/3373441

- két hálózat-típus definiál, melyet Transition Security Network (TSN) és Robust Security Network (RSN) névvel láttak el
- új adattitkosítási és integritási metódusok bevezetése: Temporal Key Integrity Protocol (TKIP) és Counter mode/CBC-MAC Protocol (CCMP)
- új hitelesítési mechanizmusok az EAP felhasználásával
- biztonsági „kézfogás” (security handshake) protokollok a 802.1x szabvány felett a kulcsmenedzsment megvalósításához

A 802.11i szabvány hitelesítési és hozzáférés-vezérlési modelljét a 802.1x szabványból kölcsönözték, azzal a követelménnyel kiegészítve, hogy a hitelesítés során egy kulcsot kell létrehozni további védelmi célokból. A 802.11i szabvány hitelesítési folyamata az EAP protokollt használja. A hitelesítő és a hitelesítő szerver közötti kommunikációra az RSN a RADIUS protokollt ajánlja.

A 802.11i szabvány bevezetéséig mindössze egyetlen titkos kulcs létezett a hitelesítésre és az adattitkosításra, azonban új kulcskezelési és generálási hierarchiát vezettek be a kulcsok rendszeres időközönkénti cseréjéhez, így csökkentve a támadó esélyeit. A kulcs hierarchia a következőképpen néz ki:



4. ábra: Kulcshierarchia a 802.11i protokollban

Forrás: http://kutfo.hit.bme.hu/oktatas/802.11i_meres.

Az MK (Master Key) az a titok, melyet a kliensnek és a hitelesítést végző eszköznek egyaránt 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 AP-nak, mely ezután engedélyezi a 802.11 csatornán a kommunikációt. A PMK-ból 4-utas-kézfogással generál a kliens és az AP ideiglenes kulcsot (PTK – Pairwise Transient Key), mely a PMK-ból származik és 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) feladata a PMK egyezésének vizsgálata az AP és a kliens között, így akadályozva meg a kulcs meghamisítását. A kulcskódoló kulcs (KEK – Key Encryption Key) célja csoportos átmeneti kulcs (GTK – Group Transient 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, de 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 ("Ron's Code" 4) vagy CCMP (AES-CCM – AES – Counter Mode Encryption) algoritmusokkal.[22]

4.3.2. Titkosítási protokollok

A 802.11i szabványban foglalt változtatásokkal együtt három titkosítási protokoll áll rendelkezésre a 802.11 szabványban: WEP, TKIP, AES-CCMP. Ezek a protokollok több feladatot is ellátnak: bizalmasság biztosítása; üzenet integritásának megvédése.

WEP

A WEP (Wired Equivalent Privacy, Vezetékessel Egyenértékű Titkosítás) a kezdeti Wi-Fi szabványok biztonsági technológiája. A WEP-et eredetileg WLAN kapcsolatok titkosítására találták ki.

A WEP tervezésénél három dologra törekedtek:

- szállítás közben megelőzni a csomagok tartalmának láthatóságát

[22] http://kutfo.hit.bme.hu/oktatas/802.11i_meres

- szállítás közben megelőzni a csomagok tartalmának módosítását
- hozzáférés-vezérlés biztosítása a hálózathoz[23]

A WEP protokoll az RC4 titkosító algoritmusra épül, mely 40 vagy 104 bites kulcsot használ kombinálva a 24 bites inicializáló vektorral (IV). Az RC4 folyamkódoló algoritmus a titkos kulcsból és egy véletlen számból álló véletlen bájtsorozatot állít elő, amelyet XOR-ol az üzenet bájtjaival. A kulcsok a szabvány szerint 40 bitesek, de a mai hardverek gyakorlatilag kivétel nélkül támogatják a 104 bites hosszúságú változatát. Az IV fontos része a titkosításnak, mert segítségével az RC4 algoritmus mindig más titkosító kulcsot használ. A kulcsot, mint nyílt szöveget (plain text) küldik oda vissza a hálózaton a kommunikációban résztvevő eszközök, ráadásul mindegyik eszköz ugyanazt az egyetlen kulcsot használja. A 64 bites (40 + 24 bit) WEP kulcsszó visszafejtéséhez napjainkban pár perc, és nagyjából 40000 adatcsomag vizsgálata elegendő. Alkalmazása bizonyítottan nem megfelelő a hálózat védelmére, így használata önmagában nem javasolt. (Sankar et al. [2004])

A WEP eljárást vizsgálva az alábbi hiányosságokat szokták megemlíteni[24]:

- Ugyanazt a kulcsot használja hitelesítésre és kódolásra, így kulcs megszerzése esetén minden üzenet visszafejthető.
- A hitelesítés csak a hálózathoz való csatlakozás pillanatában történik és többet nem
- Nincs kölcsönös hitelesítés, csak a kliensnek kell hitelesítetnie magát, az AP-nek nem.
- Statikus kulcsokat alkalmaz, így nagy rendszerben sok időt igényel a kulcsok cseréje
- WEP 128 bites titkos kulcsa valójában 104 bites, mert 24 bit nyíltan kerül átvitelre
- A 24 bites IV összes lehetséges száma 2^{24} = 16 777 216, ami az ismétlődések gyakoriságát tekintve kicsi szám.
- Léteznek gyenge RC4 kulcsok, melyekből az RC4 algoritmus nem teljesen véletlen bájtsorozatot állít elő. Ilyen gyenge kulcsból előállított bájtsorozat első néhány bájtját megfigyelve lehet következtetni a kulcsra.

TKIP

A WEP hibái miatt megalkották a TKIP protokollt (Időszakos Kulcs Sérthetetlenségi Protokoll), mint egy köztes biztonsági protokollt a WEP és egy sokkal biztonságosabb

[23] http://ciscobook.org.ua/cisco_wireless_lan_security/ch08lev1sec2.html

[24] http://alpha.tmit.bme.hu/meresek/wlan.htm

protokoll (AES-CCMP) között. A később elfogadott WPA2 a TKIP mellett tartalmazza és megköveteli az AES titkosítást. A bizottságnak biztosítani kellett a visszafelé való kompatibilitást, ezért a WPA a TKIP titkosítást használja (nem kellett a meglévő hardvert fejleszteni).[25] A TKIP-be beépítettek egy üzenetintegritás ellenőrzést is, ami CRC-32-es ellenőrzőösszeg számítását kiegészíti a Michael algoritmussal, amely biztosítja az integritást a kisteljesítményű processzorokon is. A Michael egy 64 bites MIC-et (Message Integrity Code) számol, amelyet a TKIP titkosítva küld el. A TKIP titkosítási mód kiküszöböli a WEP esetében előforduló ismétlődő IV előfordulását a hossz 24 bitesről 48 bitesre emelésével. A TKIP a 802.11i kulcsmenedzsment modelljére épül. A TKIP az IV értéket számlálóként is használja, így véd a visszajátszásos támadással szemben, továbbá az RC4 kulcsokat minden keretnél megváltoztatja.[26] A TKIP protokoll sem teljesen biztonságos: japán tudósoknak sikerült egy perc alatt feltörni a WPA-TKIP titkosítást[27]. A TKIP protokoll gyengeségei: négy-utas kézfogás; támadás a Michael algoritmus ellen; támadások a PSK (pre-shared key) felhasználásával; a temporal key hash gyengeségeinek kihasználása.[28]

AES-CCMP

A 802.11i szabvány másik titkosítási protokollja a CCMP (Counter Mode/CBC-MAC Protocol), mely az RSN központi részét képezi. A CCMP erősebb titkosítási algoritmus, mint a TKIP és szintén biztosítja a bizalmasságot, integritást és a visszajátszás ellen védelmet. A CCMP alapja az AES blokkrejtjelező szabvány, mely egy nemzetközi verseny eredményeképpen születetett meg a már elavult DES (Data Encryption Standard) szabvány leváltására.[29] A CCMP titkosítási protokoll megszabadult az RC4 protokolltól és az AES CRT (Counter) mód és a CBC-MAC (Cipher Block Chaining – Message Authentication Code) kombinációjából megalkotta a CCMP-t (Counter with CBC-MAC). A CCMP a CTR-t (counter mode) használja a bizalmasság, míg a CBC-MAC-et az integritás biztosítására. (Sankar et al. [2004]) Az AES nemzetközileg elismert szimmetrikus titkosítási szabvány, mely lehetővé teszi a változó kulcs- és blokkméret alkalmazását. A CCMP 128 bites kulcs- és blokkmérettel dolgozik. CCMP módban, az üzenet küldője először kiszámolja az üzenet

[25] http://ciscobook.org.ua/cisco_wireless_lan_security/ch08lev1sec2.html

[26] http://www.hiradastechnika.hu/data/upload/file/2006/2006_5/HT_0605.pdf

[27] http://index.hu/tech/2009/08/28/egy_perc_alatt_feltorheto_a_wifi/

CBC-MAC értékét, ezt az üzenethez csatolja, majd az üzenetet CTR módban rejtjelezi. A CBC-MAC számítás kiterjed az üzenet fejlécére is, a rejtjelezés azonban csak az üzenet hasznos tartalmára és a CBC-MAC értékre vonatkozik. A CCMP mód tehát egyszerre biztosítja a teljes üzenet (beleértve a fejlécet is) integritásának védelmét és az üzenet tartalmának titkosságát. A visszajátszás ellen az üzenetek sorszámozásával védekezik a protokoll. A sorszám a CBC-MAC számításhoz szükséges inicializáló blokkban van elhelyezve.[28]

Cisco protokollok és a WPA

A 802.11i szabvány megvalósulása hosszú időt vett igénybe (2001-2004). Azonban gazdasági és üzleti okok miatt a 802.11i szabványnak számos változata lett. A Cisco kifejlesztette a CKIP (Cisco Key Integrity Protocol) protokollt, ami a TKIP Cisco féle változata. A CKIP egy sorszámot alkalmazott a WEP kulcs csomagonkénti változásának biztosításához. A Cisco MIC (Message Integrity Check) erősebb védelmet nyújt, mint a Michael algoritmus. A Cisco kifejlesztett egy kulcskezelési eljárást a CKIP részeként. A CKIP (a 802.11i szabvánnyal ellentétben) esetében a kulcs az AP által kerül meghatározásra, majd EAPoL-Key csomag formájában lesz elküldve, így kliens oldalon könnyebb implementálni. Ezen újításokkal a Cisco gyorsan javította a WEP biztonsági hibáit. A WPA a 802.11i szabványtervezet része, melyet a Wi-Fi Szövetség fejlesztett ki. A szövetség igyekezett az IEEE-nél hamarabb megoldást találni és megőrizni a kompatibilitást a 802.11i szabvánnyal. Amikor a 802.11i szabványtervezetet elfogadták a Wi-Fi szövetség a WPA2 elnevezést adta neki. A WPA egy korai (v3.0) 802.11i szabványtervezeten alapul és elsődlegesen a TKIP protokollt, a 802.1x hitelesítést és a kulcsmenedzsmentet implementálta, illetve lecserélte a nyílt kulcsú és a hibás osztott-kulcsú hitelesítést. A WPA-t és a WEP-et vegyesen használó módszert *kevert módnak* nevezzük, melynek biztonsága megkérdőjelezhető a WEP biztonsági hiányosságai miatt. A WPA és WPA2 a különböző 802.1x specifikációk miatt nem tud együttműködni. (Sankar et al. [2004])

[28] http://www.crysys.hu/publications/files/ButtyanD06ht.pdf

5. Támadási módszerek ismertetése

A vezeték nélküli hálózatok különösen támadhatók, mivel nehéz megakadályozni a fizikai hozzáférést. A piacon kapható antennák segítségével egy támadó akár kilométeres távolságból is küldhet és fogadhat jeleket. A vezeték nélküli hálózatok biztonságát csak úgy lehet garantálni, ha ismerjük a támadási típusokat és a hálózat gyenge pontjait. A vezeték nélküli hálózatok passzív (a támadó csak a jeleket fogja) és aktív (a támadó is küld jeleket) támadásoknak vannak kitéve. Előbbit nagyon egyszerű kivitelezni, mert elég egy vezeték nélküli antenna, ráadásul a támadás még észrevétlen is marad. Minden jó biztonsági mechanizmus azon a feltételezésen alapul, hogy a támadó mindent lát! (Sankar et al. [2004])

5.1. A támadó céljai

Egy támadónak számos oka lehet egy vezeték nélküli hálózat megtámadásához. Lehet, hogy csak a hálózat erőforrásaihoz akar hozzáférni pl. bizalmas dokumentumokhoz. Számos szervezet és vállalat csak a hálózat legkülső rétegének védelmét tartja szem előtt, így a belülről érkező támadásokkal szemben sokkal érzékenyebb. Egy vezeték nélküli hálózat talán könnyű célpont lehet a belső emberek számára, ha nincs megfelelő védelemmel ellátva. Más támadók lehet, hogy csak a vezeték nélküli hálózatot használják az Internet eléréshez (pl. repülőtéren). A támadónak célja lehet akár a hálózatot kéretlen levelek szétküldésére használni (anonimitása biztosítva van) vagy a legújabb féregprogram (worm, badware, trójai, stb.) kiindulási pontjának választhat egy hálózati gépet. A támadó akár az összes gépet felhasználhatja egy zombi-hálózat létrehozásához (pl. DDoS támadáshoz). A támadók leggyakoribb célja az olvasási vagy írási jog (hozzáférést) megszerzése a hálózaton belül. Az olvasási joggal a hálózati adatforgalmat összegyűjthetik és támadást indíthatnak a hitelesítés, titkosítás és egyéb védelmi mechanizmusok ellen. Az írási joggal csomagokat lehet küldeni az állomásoknak (olvasási jog is szükséges, ha az állomás válaszol). Egyes esetekben a támadó csomagokat küldhet a hálózatba úgy, hogy dekódolni tudna bármilyen visszajövő forgalmat. (Sankar et al. [2004])

5.2. Felderítési támadások

A vezeték nélküli hálózat egyik legnagyobb biztonsági problémája, hogy a rendszer nem zárt, mint pl. a vezetékes hálózat esetében. A rádiójelet nem állítja meg a fal, így a támadók elfoghatják az RF jeleket és küldhetnek is megfelelő távolságon belül. A felderítés célja: meghatározni a megfelelő célpontot és analizálni a célpont által futtatott biztonsági mechanizmusokat, felderíteni a célpont gyenge pontjait és ezek alapján kiválasztani a támadáshoz leginkább megfelelő eszközt. A *lehallgatás* (*sniffing)* egy általános hálózati kifejezés, mely bármilyen átviteli közegen továbbított csomag elfogását jelenti. Ha ez a médium a levegő, akkor ez a folyamat nagyon egyszerű és még észrevétlen is. A piacon találhatunk fizetős sniffer programokat is, de a legtöbb ingyenes program segítségével is lehetőség van tetszőleges csomag elküldésére (packet injection). Az SSID-t gyakran gondolják biztonsági mechanizmusnak, azonban az SSID egy metódus a vezeték nélküli hálózatok megkülönböztetésére. A jelzőkeretek formájában (beacon) szórt SSID-t a különböző sniffer programok (pl. NetStumbler, Kismet) megjegyzik. A legtöbb eszközben tiltani lehet az SSID szórását, de ez csak megnövekedett forgalmat eredményez a menedzsmentkeretek miatt, s biztonsági szempontból nem jelentős előrelépés.

A legjobb módszer arra, hogy megtudjuk, mi történik a hálózaton a lehallgatás. A hálózati forgalom lehallgatása mind a támadóknak, mind pedig a hálózatot védőknek fontos. A sniffer programoknak két fő funkciójuk van: csomagok elfogása és a hasznos csomagok analizálása, megjelenítése. Néhány nyílt forráskódú program csak az előbbi funkcióval rendelkezik, de a legtöbb ilyen program képes valamilyen szintű (vizuális) megjelenítésre. A csomagelemzés kulcsfontosságú eszköz a támadó kezében. A hálózati rendszergazda egy felderítési támadással ellenőrizheti az általa felügyelt hálózat biztonságát és beállításait.

A *wardriving* nem más, mint adott területen statisztika készítése a területen elérhető vezeték nélküli hálózatokról. Ezt legegyszerűbben egy autóból tehetjük meg. A wardriving egyre népszerűbb napjainkban annak ellenére, hogy lopásnak minősül[29] és számos, Internetről ingyenesen letölthető program áll rendelkezésre ahhoz, hogy feltérképezzük a nyitott Wi-Fi hálózatokat. A legismertebb programok a Network Stumbler, Kismet, stb. Ezek a programok a legtöbb vezeték nélküli hálózati kártyával együttműködnek. (Sankar et al. [2004])

[29] http://www.origo.hu/techbazis/internet/20071129-a-szabad-wifihasznalat-lopasnak-minosul.html

5.3. DoS támadások

A szolgáltatásmegtagadás (továbbiakban DoS) egy adott szolgáltatás működésének megakadályozására utal. Ez az akadályozás lehet akár hálózati eszközök fizikai rongálása, tönkretétele, de a támadó lefoglalhatja a maximális sávszélességet, ezzel megbénítva a szolgáltatást. A vezeték nélküli hálózatok esetében a DoS különösen nagy probléma, mert az átviteli közeg bárki számára elérhető és pl. egy rádiós interferenciát gerjesztő eszközzel (jammer) blokkolható akár az egész hálózat.

Diszasszociációs és deauthentikációs támadások

A 802.11 menedzsment-keretek nincsenek hitelesítve ezért a diszasszociációs és deauthentikációs támadások keretében az állomás csatlakozáskor elsőnek hitelesítési, majd asszociációs kereteket küld. Az állomás csak azután tud a hálózatban található többi állomással kommunikálni, ha asszociált az AP-hoz. Azonban bármelyik állomás hamisíthat kereteket és küldhet diszasszociációs és deauthentikációs üzeneteket az AP-nak. Ennek hatására az AP diszasszociálja az adott állomást, melynek újból végig kell menni a hitelesítési és asszociációs folyamaton. Ha a támadó ismétlődően küld ilyen kereteket, akkor állomásokat akadályozhat a hálózathoz való hozzáférésben. A támadás egyik implementációja az Omerta program, mely figyelemmel kíséri a hálózatban található összes üzenetet és egyszerűen minden érzékelt keret után küld egy diszasszociációs üzenetet. Az *AirJack* programcsomag *essid_jack* nevű része egy hitelesített és az AP-hoz asszociált állomást diszasszociál, minek hatására a felhasználó küld egy próbakeretet, amiben az SSID titkosítatlanul szerepel, így a támadó hozzájut a rejtett SSID-hoz. Ebből is kitűnik, hogy az SSID szórásának tiltása miért nem igazi biztonsági mechanizmus. Ezt a módszert használják ki a PEAP protokoll man-in-the-middle (MitM) típusú támadásakor: a támadó nem engedi az állomás hálózathoz csatlakozását, mert ő lép a helyébe. A *money_jack* támadás deauthentikál egy felhasználót és a támadó az AP-nak adja ki magát. Ha nincs kölcsönös hitelesítés, az állomás akár fontos információkat is kiadhat. A *void11* program az AP asszociációs tábláját támadja, úgy, hogy állandóan hitelesítési kéréseket küld a támadó. Ezért az AP asszociációs táblája megtelik, így szolgáltatás-megtagadás jön létre. (Sankar et al. [2004])

5.4. Hitelesítési támadások

A DoS támadások egyszerűek, de csak bizonyos célokra használhatóak. Az eredeti 802.11 szabvány egy elég gyenge hitelesítési mechanizmust specifikált arra, hogy melyik állomás csatlakozhat a hálózathoz. Az IEEE azonban újabb hitelesítési eljárásokat vezetett be, melyek alapjai a 802.1x szabvány és az EAP protokollok.

Osztott-kulcsú hitelesítés támadása

A 802.11 szabvány tervezői megalkottak egy hitelesítési mechanizmust, az osztott-kulcsú hitelesítést, amit azonban könnyű kijátszani. Az osztott-kulcsú hitelesítés opcionális. Az alapértelmezett hitelesítési mód a nyílt hitelesítés (megfelel annak, hogy nincs hitelesítés), azonban mind a kéttípusú hitelesítésnél hatékonyabb az EAP alapú hitelesítés. Az osztott-kulcsú hitelesítés egy kölcsönös hitelesítési mechanizmus, melyben mindkét fél egy véletlenszerű kihívást (challenge) küld, melyet mind a két fél titkosít és a titkosított kihívás elküldésével bizonyítja, hogy ismeri a WEP kulcsot. A támadó elég információt szerezhet egy egyszeri sikeres hitelesítés megvizsgálásából ahhoz, hogy az így szerzett információkat felhasználva sikeres hitelesítési válaszokat küldhessen. A kihíváson és a válaszon XOR műveletet alkalmazva a támadó kitalálhatja az adott IV-hez (inicializáló vektor) tartozó kulcssorozat egy részét. Ezután a kiszámított kulcs segítségével és az elfogott IV ismételt használatával sikeresen átmehet a hitelesítési eljáráson.

MAC-cím hamisítás (MAC-cím spoofing)

Számos eszköz biztonsági beállításként kínálja a MAC-címszűrést, melynek konfigurálása sok időt vesz igénybe és a konfiguráció során könnyű hibát ejteni. Az alapvető probléma az, hogy egy támadó egyszerűen meg tud hamisítani egy MAC-címet. Egyes NIC illesztőprogramok felkínálják ezt a lehetősége, de ennek hiányában számos ingyenes program található az Interneten a MAC-cím megváltoztatására (Windows: MACMeUp; Linux: macchanger). A hamisítás feltétele az, hogy legalább egy érvényes címet tudni kell, azonban mivel a címmező nem titkosított, egy keret elfogásával már meg is van a cím. (Sankar [2004])

5.5. A WEP és WPA protokollokat érintő támadások

A WEP titkosítás által használt kulcs előállításához két út vezet: megtaláljuk a kulcsot vagy megkeressük az összes olyan kulcsfolyamot, melyet egy kulcs generálhat. Az RC4 titkosítás során egy nyílt üzenetet (plaintext – P) és egy kulcsfolyamot (keystream – K) XOR-olunk össze és így kapjuk meg a titkos üzenetet (ciphertext – C). Bármelyik két elem ismeretében meghatározható a harmadik. A C mindig ismert (üzenetszórásban közli az állomás), így a P ismeretében, megfejthető a K, majd ezután minden P visszafejthető. Az RC4 biztonsága azon alapul, hogy a kulcsfolyamok nem ismétlődnek. A WEP ezt az IV (inicializáló vektor) segítségével éri el (24 bit). Az ismétlődő kulcsokat ütközésnek nevezik. Számos technika létezik a kulcsfolyam visszafejtésére (pl. nyíltszöveg támadás - known plaintext attack, ütközést felhasználó támadás) és egy kulcsfolyam-szótár megalkotásához. A kulcsfolyam-szótár tartalmazza az egy kulcshoz rendelhető összes kulcsfolyam értékét (2^{24}). (Sankar et al. [2004])

A ChopChop támadás általános működése[30]

A WEP CRC32-ellenőrzőösszeget használ a csomagintegritás megállapításához, mely az adathoz hasonlóan titkosítva utazik. Ha a titkosított adatokon módosítunk és újraírjuk a CRC-t, akkor készíthetünk olyan csomagot amit elfogad az AP. Így a kulcs ismerete nélkül felül lehet írni a WEP-csomagokat és addig lehet módosítani, amíg a titkosított CRC is helyes lesz. A módszer segítségével bájtonként meghatározhatjuk a csomag tartalmát. A teljes csomag ismeretében meghatározhatjuk a kulcsot: *(titkosítatlan változat)* XOR *(titkosított változat)*. A WEP-et használó rendszerekben a támadónak csak egy kulcssort kell injektálnia egy csomagba, mert a 802.11 szabvány szerint a küldő megválaszthatja a saját IV-jét. A szabvány nem tiltja egy korábbi IV újbóli használatát, így tetszőleges számú csomagot küldhetünk a megtalált IV-t injektálva a csomagokba. Néhány gyártó azonban (pl. Cisco) egy mechanizmust implementált (MIC - Message integrity check, üzenetintegritás ellenőrző), mely nem engedi meg az ismétlődő IV-ket.
A WEP protokoll sebezhető pontjai és az implementációs hibák miatt a támadók egyik legjobban kedvelt célpontja a WEP kulcs visszafejtése. A legkomolyabb ilyen kulcstámadás a

[30] http://ethicalhacking.hu/wpa.aspx

Fluhrer-Mantin-Shamir (FMS) támadás, mely percek alatt lehetővé teszi a passzív lehallgatás során gyűjtött csomagokból a WEP kulcs feltörését. (Sankar et al. [2004])

Szótár alapú támadások

Az erősnek mondott WEP kulcsok 104 bitesek, melyeket manuálisan adnak meg. A *wep_crack* nevű eszköz képes a jelmondat alapú jelszavak feltörésére úgy, hogy a WEP kulcsgenerátor algoritmusnak bead minden a szótárban szereplő szót. Ez működik abban az esetben is, ha a lehallgatás (sniffelés) során fájlba mentettük a csomagokat. A program először keres egy WEP-pel titkosított csomagot, majd a rendelkezésre álló szótár szavai alapján megpróbálja visszafejteni a csomagot. Ha a csomaghoz tartozó ICV helyes, a program tudja, hogy a WEP kulcs – mellyel visszafejtette a csomagot – helyes. Ebből következik, hogy ha a jelmondat szavai szerepelnek egy szótárban, akkor minden esetben feltörhető. Az a tapasztalat, hogy egy 40 bites kulcsgenerátor algoritmussal csak 2^{21} lehetséges WEP kulcsot lehet előállítani, függetlenül a jelmondat bonyolultságától és hosszától. Így mindösszesen 2 millió kulcsra korlátozódott a lehetséges kulcsok száma, melyet nyers erő (brute force) támadással akár percek alatt is fel lehet törni. (Sankar et al. [2004])

A Fluhrer-Mantin-Shamir támadás

Ez az egyik leghatékonyabb WEP elleni támadás, melynek algoritmusát Scott Fluhrer, Itsik Mantin és Adi Shamir kriptográfusok alkották meg 2002-ben. A támadás gyökere az RC4 titkosító protokoll kulcsütemezési algoritmusában (KSA) van, mely az RC4 első lépése. A KSA a kulcsot egy mátrixszá transzformálja és ebből generálja az RC4 a kulcssort. A hiba egy statisztikai anomália, mely kimondja, hogy ha adott kulcsokat bizonyos módon strukturálunk, akkor a kulcsok egy része nagyobb valószínűséggel kerül a kulcssor végére, mint más kulcsok. A támadás során nagy mennyiségű titkosított adatot kell gyűjteni, majd meg kell keresni azokat a csomagokat, amelyekben a kulcs struktúrája gyenge (ún. hasznos csomagok). Kb. 4-6 millió ilyen csomagra van szükség a kulcs meghatározásához.
Az FMS algoritmust továbbfejlesztve 2004-ben napvilágot látott a Korek's WEP Attack program[31], mely szintén statisztikai támadást végez, de a támadás során már 500.000–2.000.000 csomag is elegendő (104 bites WEP kulcs esetén). 2007-ben megalkották a PTW-t

[31] http://www.oxid.it/ca_um/topics/wep_cracker.htm

(Pyshkin, Tews, Weinmann), a WEP-et minden eddiginél hatékonyabban feltörő támadást, mely a 104 bites WEP kulcsot kevesebb, mint 1 perc alatt feltöri[32]. Az algoritmus használatával az estek 50%-ban kevesebb, mint 40.000 csomag elegendő volt a 104 bites kulcs meghatározásához. Ezen csomagok IV-je tetszőlegesen megválasztható. Az FMS algoritmust számos programban implementálták, mely közül a *WEPCrack* volt az első. A másik ismertebb program az AirSnort, melyet sokkal könnyebb kezelni, mint a WEPCracket. Az AirSnort az FSM egy részét implementálja a kulcstöréshez. (Sankar et al. [2004]) A WEP kulcstörés gyakorlati bemutatására a 6 . fejezetben kerül sor.

ChopChop támadás WPA ellen[33]

A vezeték nélküli hálózatokon már régóta ajánlott a WPA (Wireless Protected Access) használata, ami két féle módon konfigurálható: PSK (pre-shared key – előre egyeztetett kulcsok) vagy RADIUS használatával. [34] A 4. fejezetben tárgyaltak alapján a TKIP-et használó WPA-ban megmaradt az RC4 kódoló algoritmus és hibadetektálásként az Integrity Check Value (CRC32). Ezek együttesen lehetővé teszik a ChopChop-támadás alkalmazását. A WPA-ban az ICV-t kiegészíti a MIC (Message Integrity Check). A TKIP esetében létrehoztak egy „szekvenciális számolót", mely a fogadó félnél a csomagok sorrendjére figyel. s minden érkező csomag hatására eggyel nagyobb lesz az értéke (a nagyobb számlálóérték miatt nem lehet csomagot újraküldeni). A szabvány rögzíti, hogy ha 2 db MIC hiba fordul elő egy percen belül, akkor leáll a kapcsolat, és egy 60 másodperces szünet után indítja csak el az AP új kulccsal a kapcsolatújrafelvételi-kérelmet a kliens felé. A biztonsági mechanizmus kiküszöbölésére a támadónak a QoS (Quality of Service) Wi-Fi-be integrált megoldása áll rendelkezésére. QoS esetében egy adott csatorna nyolc alcsatornára van felosztva, így a kommunikáció során egy eszköz a csatornán belül egy másik alcsatornára válthat a jobb átviteli minőség eléréséhez. Minden alcsatornához egyedi számláló tartozik, de a kliensek szinte mindig csak a nullás alcsatornát használják, így majdnem mindig található olyan alcsatorna, ahol alacsonyabb a számláló értéke, ezért a módosított csomagot elfogadja az AP. A WPA kompatibilitása miatt először az ICV-ellenőrzés fut le, és ha ez rendben van, akkor

[32] http://eprint.iacr.org/2007/120

[33] http://ethicalhacking.hu/wpa.aspx

[34] http://docs.lucidinteractive.ca/index.php/Cracking_WEP_and_WPA_Wireless_Networks

következik a MIC-ellenőrzés. A ChopChop által használt, hibás ICV-kre épülő visszafejtés egy másik csatornán folytatódhat.
A módszerrel percenkét egy bájtot találhatunk ki, így tetszőleges csomag esetében 8 perc alatt ki tudjuk találgatni a MIC (8 bájt) titkosítatlan értékét. A megfordított Michael algoritmusnak (a függvényt kétirányúnak tervezték) szüksége van még egy titkosítatlan szövegre, és így lehet megkapni a titkosításhoz használt MIC kulcsot. Titkosítatlan szöveget legkönnyebben ARP csomag felhasználásával kaphatunk. Az ARP csomagban IP-címek és MAC-címek vannak, melyből kedvező esetben majdnem mindent ismer a támadó: MAC-címeket, az IP-címtartományt. Mindössze két bájtot nem ismer: a két IP-cím utolsó bájtját, amit két ChopChop támadással kitalál, és meg is van a teljes titkosítatlan szövege egy WPA-val titkosított csomagnak! A kapott kulcsfolyammal a támadó kódolhat egy csomagot, de a számláló értékén nem változtathat. A megoldás: addig keres megfelelő QoS csatornát, míg nem talál egy megfelelően alacsony számlálójút. A 0-son a célkliens kommunikál, így marad ideális esetben 7 csatorna a saját csomagok sugárzására. A támadó nem tudja elolvasni az átküldött tartalmat, de pl. egy ARP mérgezéssel (ARP poisoning) véghezvihet egy man-in-the-middle támadást. Ha a támadónak sikerülne mindkét irányban érvényes MIC kulcsot szereznie (ez a támadás ugyanis csak az AP-kliens irány MIC kulcsát fedi fel) és egy valós kulcsfolyamot az egyik QoS csatornára (a counter szempontjából kedvezőre) akkor bármilyen tartalommal bármennyi csomagot küldhet a hálózatnak.
A WPA titkosítási protokollnál a védekezést a rekeying intervall alacsony értékre állításával (pl. 120s) érhetjük el, így a támadó csak 1, maximum 2 bájtját szerezheti meg a MIC-nek, és a kulcsok máris kicserélődnek.

5.6. EAP protokollokat érintő támadások

Minden EAP protokollra épülő protokoll estében szükséges egy AS és egy – a leggyakrabban csak a hitelesítési üzeneteket közvetítő – AP. A támadó alkalmazhat passzív támadást (forgalom figyelése, információk gyűjtése) vagy aktív támadást (egyik részvevője a hitelesítési folyamatnak). Résztvevőként a támadó egy man-in-the-middle támadás keretében megpróbálja megszemélyesíteni a klienst vagy a szervert, esetleg mindkettőt. A MitM támadás rendszerint aktív támadásra utal, melyben a támadó két fél között helyezkedik el. Egy szerver megszemélyesítéséhez a támadó beüzemel egy hitelesítő kereteket fogadni képes AP-t

és egy háttérben futó hitelesítő szervert (a kettő lehet egy Linux szerveren is). A 802.1x hitelesítési folyamata általánosan a következőképpen néz ki (Sankar et al. [2004] 151. old):

1. A kliens hozzáférést igényel a hálózathoz.
2. Az AS és a kliens között üzenetcsere történik a hitelesítés érdekében (a hitelesítés lehet egyoldalú, vagy kölcsönös).
3. Ha az AS elfogadja a kérelmet, utasítja az AP-t, hogy engedélyezze a hozzáférést.
4. Opcionálisan az AS további információkkal szolgál az AP-nak.

A LEAP protokoll a kliens és az AS hitelesítésére az MS-CHAPv1 protokoll egy módosított változatát használja. Az AS egy kihívást küld el a visszajátszás megakadályozására, majd a kliens egy számítást végez a kihíváson és a jelszón, így biztosítva azt, hogy ismeri a helyes jelszót. PEAP protokollnál a kliens és az AS egy titkosított csatornát állít fel és a lehetséges hitelesítési folyamatok közül egyet végrehajt a csatornán. (Sankar et al. [2004])

LEAP szótár alapú támadása

A LEAP Cisco által bejegyzett protokoll, melynek gyenge pontja az MS-CHAPv1 használata. A LEAP az MS-CHAPv1 protokollt titkosítatlanul használja és védtelen az offline szótár alapú támadással szemben. A támadónak először le kell hallgatnia a LEAP hitelesítés által igényelt kihívást és választ, majd a szótárban megpróbálja megtalálni a megfelelő választ (response) a kihívás (challange) alapján. Ha ez megvan, akkor megtalálta a jelszót is és sikeresen eljátszhat egy LEAP-et használó klienst. A LEAP jelszó lehet, hogy azonos más hálózati jelszavakkal pl. a tartományi (active directory) jelszóval, ezáltal a támadó számára lehetőség nyílik a hálózat további részeinek eléréséhez. Több LEAP támadást végző programot is írtak, ilyen pl. az *asleap*. A szótártámadás elleni legjobb védekezés az erős jelszavak használata és az ezt megkövetelő biztonsági házirendek betartatása. A jelszavakat rendszeres időközönként cserélni kell. Ez az időköz erősen függ a helyi biztonsági követelményektől. Egy erős jelszó legalább 12 karakterből áll és a következők közül legalább hármat tartalmaz: kisbetű, nagybetű, szám, speciális karakter (írásjelek, ékezetes betűk)[35].

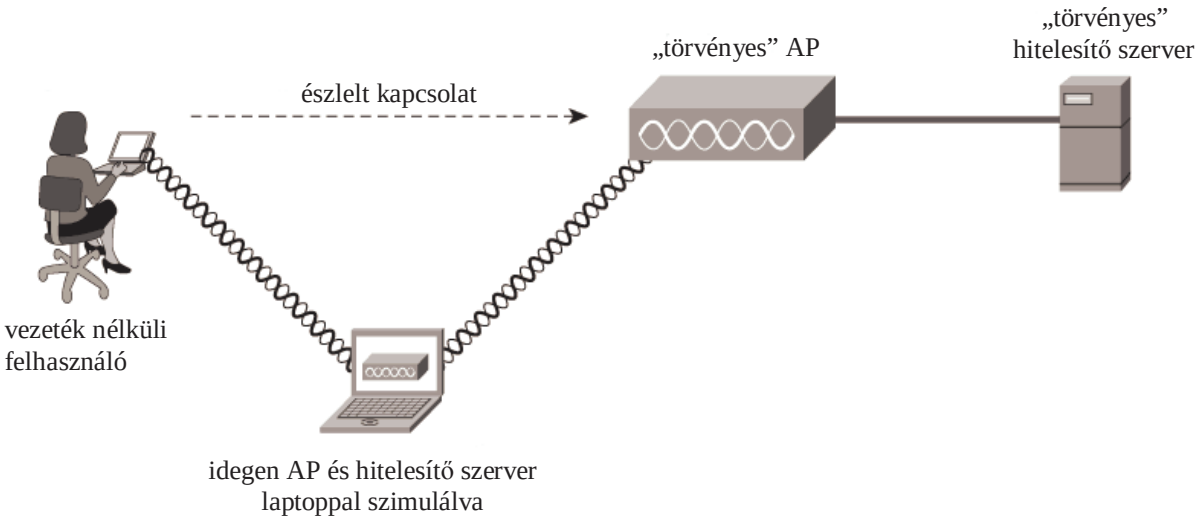
[35] http://ciscobook.org.ua/cisco_wireless_lan_security/ch06lev1sec7.html

PEAP man-in-the-middle támadás

A PEAP (Protected Extensible Authentication Protocol version 1, PEAPv1) biztonsága a következő két szabályon múlik (Sankar et al. [2004] 153. old):

- A kliensnek jóvá kell hagynia a szerver tanúsítványát.
- A belső, védett hitelesítési eljárásnak nem szabad a PEAP-en kívül, a támadó által lehallgatható módon zajlania.

Ha ezek közül bármelyiket is figyelmen kívül hagyják a PEAP biztonsága nem garantált. Így, ha a kliens nem hagyja jóvá (validate) a szerver tanúsítványát, akkor a támadó felállíthat egy idegen AP-t és AS-t, és ellophatja a kliens bejelentkezési információit. Ezután ezeket az információkat felhasználva a valódi szerver sikeresen hitelesíti. Ha a kliensalkalmazás rosszul van megtervezve vagy rosszul van konfigurálva és a belső PEAP hitelesítési információkat használja fel egy nem védett hálózati protokollban, akkor megszegi a második követelményt. Ezáltal a támadó megszerezheti a jelszót és sikeresen hitelesítheti magát a PEAP hitelesítési folyamatban. Az 5. ábrán a vezeték nélküli man-in-the-middle támadás általános koncepciója látható. Ezen az ábrán a laptop idegen AP-t szimulál, mely egy közbülső emberként van jelen a hálózatban: elfogja a felhasználói adatokat, majd azok felhasználásával hozzáférhet a valós hálózathoz. A támadó továbbíthatja is a felhasználó forgalmát és így észrevétlen maradhat a támadás egy ideig. Az észlelt kapcsolat alatt a felhasználó által érzékelt kapcsolatot értjük.



5. ábra: Vezeték nélküli MitM támadás általános koncepciója.

Forrás: Sankar et al. [2004] 153. old

Általánosan elmondható, hogy jobb a felhasználóknak nem megengedni az érvénytelen szervertanúsítványok elfogadását. A felhasználók általában nem tudják eldönteni egy tanúsítványról, hogy az igazi-e vagy önmaga által aláírt. Minden olyan konfigurációs lehetőség, melyben lehetőséget adunk a naiv felhasználóknak egy „Igen" megnyomására, csökkenti a PEAP biztonságát. Az EAP-TTLS a fenti két követelményt szabja meg és hasonlóan támadható a MitM támadással, ha ezeket a követelményeket figyelmen kívül hagyják. A PEAP 2-es verziójában a MitM támadást úgy próbálják kivédeni, hogy kriptografikailag összerendelik a belső EAP metódust a külső csatornával. Így a belső hitelesítést nem lehet csak védett menetben (session) futtatni. (Sankar et al. [2004])

5.7. Idegen hozzáférési pontok

Idegen hozzáférési pontnak (rouge AP) a hálózatban található nem hitelesített, azaz nem az üzemeltető által kezelt AP-kat nevezzük. A hálózati felhasználók gyakran állítanak fel idegen hozzáférési pontokat pl. a vezeték nélküli infrastruktúra hiányában, ami azonban súlyos következménnyel jár(hat), ugyanis a megfelelő biztonsági beállítások elmulasztásából fakadóan komoly biztonsági rés keletkezik a hálózatban. Nagy veszélyt jelentenek a boltokban kapható hozzáférési pontok, melyek könnyű beállítással kecsegtetik a felhasználót, azonban a biztonsági szempontokat is ilyen könnyedén mellőzik. Idegen hozzáférési pontot egy támadó is elhelyezhet, akár az épületen kívül is pl. egy furgonban vagy egy szomszédos épületben. Az előzőekben ismertetett man-in-the-middle támadás feltétele, hogy a támadó egy idegen AP-t helyez el a hálózatban.

Az Airsnarf programmal a nyilvános AP-k (pl. reptereken, szállodákban) adatforgalmát lehet gyűjteni oly módon, hogy egy idegen AP-t helyezünk az eredeti AP közelébe, így az idegen AP-hoz csatlakoznak a felhasználók. A program a felhasználó által kért weboldalt hozza be. Ha a felhasználó nem vesz igénybe olyan szolgáltatást (pl. SSL-t használó szolgáltatás), mely hitelesíti az AP-t, akkor nem tud védekezni a támadással szemben. A támadás ellen részben védenek az egyszeri jelszavak (OTP), azonban nem megoldás ez sem, mert a támadó egy munkamenet (session) idejéig használni tudja a megszerzett adatokat. A támadó akár egy hamis fizetési oldalt is felállíthat, ahol bankkártya számokat és egyéb érzékeny adatokat gyűjthet. Idegen AP segítségével egy támadó a maga által elhelyezett AP-ról indít támadásokat és az adatokat azon keresztül juttatja ki a hálózatból. (Sankar et al. [2004])

6. Vezeték nélküli hálózatok támadásának szimulálása

6.1. A teszthálózat és a tesztelési célok bemutatása

A vezeték nélküli hálózatok teszteléséhez és a támadások szimulálásához az alábbi eszközökből álló teszthálózatot építettem ki:

- 1 db AP, mely egyben egy DHCP szerver is és ez az alapértelmezett átjáró
- 2 db laptop, melyből az egyik a támadót, a másik az áldozatot szimulálja

A támadó gépének megfelelő laptopon az ingyenesen letölthető BackTrack3 linux live disztribúciót[36] használtam. A BackTrack (BT) több éves múltra tekint vissza és az alapja egy SLAX linux disztribúció. A program több formátumban elérhető: CD-képfájl formátumban, USB verzió és VmWare virtuális gép formátumban. Az áldozatot megszemélyesítő állomáson Windows XP operációs rendszer található, mely FTP szolgáltatást nyújt.

A tesztelés célja a támadó szemszögéből bemutatni a lehetséges támadásokat és a támadásokhoz felhasznált programokat. A tesztelési folyamat a következőképpen néz ki:

- a vezeték nélküli hálózatok feltérképezése
- a feltérképezett hálózatok vizsgálata, lehetséges kapcsolatok létrehozása
- MAC alapú hitelesítés kivédése, behatolás WEP titkosítást használó hálózatba
- hálózati eszközök és szolgáltatások feltérképezésének bemutatása
- jogosultságszerzés bemutatása: man-in-the-middle támadás a gyakorlatban, FTP és egyéb jelszavak elfogása

A tesztelési folyamat során az egyes munkafázisoknál ismertetem az alkalmazott programokat.

6.2. Vezeték nélküli hálózatok támadásának lépései

A vezeték nélküli hálózatok támadása során a támadó elsődleges célja a megfelelő jogosultságok megszerzése a hálózathoz való csatlakozáshoz. A támadás folyamatát sokfelől meg lehet közelíteni pl.: a támadást megelőzheti egy social engineering (pszichomérnöki

[36] www.remote-exploit.org/backtrack.html

tevékenység[37], találóan: az emberek bizalomra való hajlamának manipulatív kihasználása[38]), melyben fontos információkat lehet megszerezni. A következőkben ismertetett és kifejtett lépések egy általános módszert mutatnak be egy vezeték nélküli hálózat megtámadásához.

A támadó első lépésben passzív lehallgatás során megállapítja valamilyen sniffer program segítségével a jelenlévő vezeték nélküli hálózatokat (SSID), a hálózati eszköz típusát (gyártó, MAC-cím), a jelerősséget, a használt szabványt, csatornát és titkosítást. A támadó a hálózatok feltérképezéséhez használhat bármilyen hordozható eszközt (laptop, PDA, speciális eszköz).

A következő lépésben a támadó eldönti, hogy melyik hálózathoz akar csatlakozni. Ha a kiválasztott hálózaton nincs titkosítás és hitelesítési folyamat beállítva, akkor a csatlakozásnak nincs akadálya. Továbbá ha a hálózatban van DHCP szerver, akkor a támadó eszköze IP-címet is kaphat az asszociáció után. Ha a támadó nem kap IP-címet, akkor valamilyen sniffer program segítségével meghatározhatja a hálózatban használt IP-hálózatot és manuálisan adhat magának IP-címet. Ha a támadónak már van IP-címe, akkor felderítheti a hálózatban található többi állomást, szervert. A felderítés során megvizsgálja a hálózatban használt szolgáltatásokat a port címek és az elfogott csomagok alapján, ezáltal felmérheti a támadási lehetőségeket. Ha a támadó a csatlakozás után IP-címet is kap DHCP-n keresztül, akkor legtöbb esetben már tudja az alapértelmezett átjáró IP-címét, melyet támadás alá vehet. Nagyon sok helyen az átjáró alapbeállításokkal van konfigurálva, így a gyári felhasználói név/jelszó párossal a támadó hozzá is férhet pl.: a vezeték nélküli AP beállításaihoz. Ha a támadó egy titkosítást és hitelesítést használó hálózatot akar megtámadni, akkor már több feladata lesz. Gyenge titkosítást használó (pl. WEP) hálózatok esetében akár 5 perc alatt hozzájuthat a kulcshoz, majd ezután csatlakozhat a hálózathoz. Ha hitelesítés is van beállítva a hálózatban, akkor az egyszerűbb hitelesítési eljárások során – mint a MAC-cím szűrés – elég a támadónak egy, a hálózatban résztvevő állomás MAC-címével csatlakoznia. Azonban bonyolultabb megoldások esetén, mint például a 802.1x és RADIUS együttes használatakor, a támadónak már komolyabb eszközöket kell bevetnie (pl. man-in-the-middle támadás), de a siker nem garantált.

[37] Thomas Hálózati biztonság c. könyvében a fordító így fordította, de általánosan elfogadott fordítása nincs.

[38] http://www.securifocus.com/portal.php?pagename=hir_reszlet&hir_id=959&i=

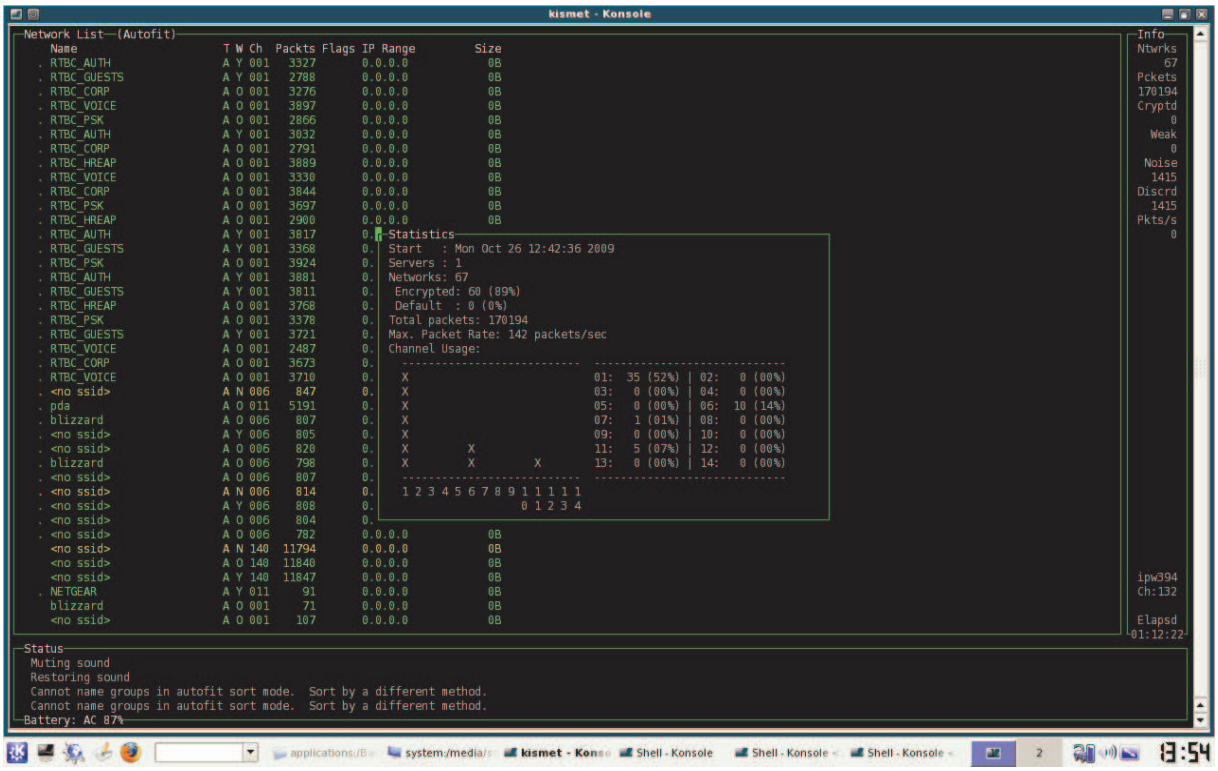
6.3. Az elérhető hálózatok feltérképezése

A legtöbb operációs rendszerben találhatunk olyan programokat, melyek megmutatják az elérhető hálózatokat, és ezek általában a hálózati kártya szoftverével együtt kerülnek telepítésre. Azonban az Internetről letölthetünk számos erre a célra írt programot, melyek általában több információt nyújtanak. Mind Windows, mind pedig Linux platformra vannak egyszerűbb és komolyabb programok. Windows platformon az egyik legnépszerűbb ilyen program a Network Stumbler, de hasonló tudású program az inSSIDer is. Közös jellemzőjük, hogy megjelenítik az elérhető hálózatokat az SSID alapján. Ezen kívül megmutatják a hálózatokhoz tartozó jelerősséget, a használt titkosítást (a NetStumbler nem tesz különbséget a WEP és WPA titkosítás között, az inSSIDer igen), az SSID-t forgalmazó eszköz MAC-címét, a hálózat típusát (Ad hoc/Infrastructure), a sebességet (11Mbps, 54 Mbps) és az utolsó érzékelés időpontját. Mindezek mellé az inSSIDer grafikont is rajzol az egyes hálózatokhoz tartozó jelerősségről, így nyomon követhető az egyes hálózatok elérhetősége.

A Linux alá írt Kismet (Apple Mac változata a KisMAC) egy vezeték nélküli hálózati detektor, sniffer és IDS rendszer. A Kismet futtatható Windows alatt is, azonban ehhez szükséges a Win32/Cygwin futtatási környezet, mely Linux környezetet biztosít a Kismet számára. A Kismet alapvetően parancssoros alkalmazás, a beállításait különböző paraméterek hozzáadásával lehet szabályozni az indítás során. A Kismet rendelkezik egy karaktergrafikus felülettel is, melyet a tesztelés során használtam. Az elérhető kapcsolókról és azok funkciójáról részletes dokumentáció a Kismet honlapján[39] található.

A Kismet elindítása után a program automatikusan megjeleníti az észlelt hálózatokat, még azokat is, melyeket a beépített Wi-Fi menedzserek (pl. Wireless Assistant a BackTrackben) nem ismernek fel (6. ábra). A hálózatokat – csak úgy, mint az előbbi Windows rendszerben futtatható alkalmazások esetében – különböző paraméterek szerint lehet rendeztetni (SSID első észlelése, jelerősség, stb.). A Kismet az előbb említett alkalmazásoknál többet tud pl.: megjeleníti a forgalmat; statisztikát csinál a forgalomból és a csatornakihasználtságból. A Kismet program hatékonysága a modulok (plug-in) használatával növelhető. A modulok segítségével az alapvető funkciókon túl például behatolást jelző figyelmeztetéseket tudunk generálni.

[39] http://www.kismetwireless.net/documentation.shtml



6. ábra: Kismet által érzékelt hálózatok listája

A BackTrackben található másik hasonló céllal írt program a Wicrawl, ami szintén egy hálózatfeltérképező szoftver, mely hasonló adatokat szolgáltat, mint az előbbi alkalmazások. Azonban a Wicrawl ezen túlmenően megpróbál minden egyes hálózathoz csatlakozni és a sikeres/sikertelen csatlakozási kísérletekből kimutatást készít. Ha a program nyílt hálózatot talál, lehetőségünk van asszociálni ahhoz a hálózathoz. A Wicrawl számos plug-in modullal rendelkezik, melyek többek közt a hálózati kulcs visszafejtését segítik (pl. aircrack-wep-cracking, cowpatty-wpa-psk-bruteforce, stb.).

6.4. Kapcsolat létrehozása

A látható hálózatok feltérképezését követően el kell indítani az asszociációs folyamatot. A tesztelés során elsőnek nyílt hálózatban vizsgáltam a kapcsolat létrehozásának folyamatát. Először a Kismet alkalmazással néztem meg a hálózatokat, majd a beépített Wireless Managerrel csatlakoztam a teszthálózathoz. Csatlakozás során – amennyiben nem nyílt hálózatról van szó – meg kell adni a kapcsolódáshoz szükséges adatokat, például a titkosítási kulcsot. Amennyiben a hálózatban nincs DHCP szerver, akkor manuálisan kell beállítani az állomás, átjáró és DNS szerver(ek) IP-címét. Amennyiben a hálózaton titkosítás van beállítva,

a támadónak fel kell törnie a titkos jelszót ahhoz, hogy csatlakozni tudjon a hálózathoz. A későbbiekben bemutatásra kerül a WEP titkosítás feltörése.

A kapcsolódást megelőzően még a feltérképezés során érdemes egy csomaganalizáló szoftverrel „belehallgatni" a hálózatba. Ekkor megtudhatjuk a hálózatban használt címeket, amennyiben az adatok nem titkosak. Amennyiben az asszociáció sikeres volt, de nem kapunk IP-címet vagy a beállított IP-címmel nem tudunk aktívan részt venni a hálózatban, akkor lehet, hogy MAC-címszűrés van beállítva. Ilyen esetben egy csomaganalizáló szoftver segítségével kereshetünk a forgalomból egy MAC-címet (lehetőleg ne az átjáró MAC-címét!), és a BT-ben található *macchanger* parancssoros programmal meg kell változtatni a hálózati kártya MAC-címét a kiválasztott MAC-címre. Ezután figyelni kell a forgalmat: ha a hálózatban DHCP osztja az IP-címeket, akkor meg kell vizsgálni, mikor jelentkezik ki egy állomás, majd annak az állomásnak a MAC-címével tudunk majd adatot forgalmazni. Amennyiben manuálisan kapják az állomások az IP-címet, akkor meg kell várni egy állomás lecsatlakozását az AP-ról. Ezt elő is lehet segíteni egy *deauthentication* támadással. Ha nem akarunk forgalomanalizáló szoftverrel bajlódni, akkor az *airodump-ng* parancssoros alkalmazás megmondja, melyik állomás melyik hozzáférési ponthoz csatlakozik.

A kapcsolat létrejöttének ellenőrzéséhez minden esetben érdemes megpingetni az átjáró IP-címét. Ha hálózati kártyánk állapotlekérése után azt látjuk, hogy nem kapunk egyetlen DNS kiszolgáló IP-címet sem, akkor a kapcsolatot a külvilággal ellenőrizni tudjuk a 4.2.2.2 nyilvános DNS szerver pingelésével. Ha a ping sikeres, tudhatjuk, hogy az átjárón keresztül elérjük az Internetet. Innentől a 4.2.2.2 IP-cím DNS kiszolgálónak való megadásával keresünk egy kevésbé terhelt, nyitott DNS kiszolgálót[40].

6.5. A WEP és WPA biztonsága gyakorlati szempontból

A 4. fejezetben ismertetésre került a WEP és a WPA titkosítási protokollok elméleti háttere. A tesztelés során megvizsgáltam, hogy gyakorlati szempontból mennyire biztonságos egy WEP vagy egy WPA titkosítást használó hálózat.

A teszthálózatban a hozzáférési ponton nyílt hitelesítést állítottam be, 128 bites WEP titkosítási kulcs használatával. A támadó gépén a következő parancssoros segédprogramokat

[40] A következő címen nyitott DNS szerverek listája található: http://www.dnsserverlist.org

használtam: airmon-ng; airodump-ng; aireplay-ng és aircrack-ng[41]. A WEP-kulcs feltörésének menete a következő:

1. Az *airmon-ng* parancs kiadásával megnézzük a rendelkezésre álló hálózati kártyákat.
2. Az *airmon-ng* programmal monitor (figyelő) módba kapcsoljuk a hálózati kártyát (jelen esetben ez az *eth1*) a következő paranccsal: *airmon-ng start eth1*.
3. Egy másik shell-ben kiadjuk az *airodump-ng eth1* parancsot, majd a kimenetet tanulmányozva a BSSID oszlopban lévő MAC-címet felírjuk (AP MAC-címe), továbbá felírjuk az AP által használt csatornát és az ESSID-t (SSID).
4. Következő lépésben a következő parancs kiadásával megkezdjük az interfészen fogadott csomagok gyűjtését egy fájlba:
   airodump-ng -c CHANNEL_NUMBER -w CAPFILE_NAME -b AP_MAC_ADDR eth1
   A *–c* kapcsoló után az előbb látott csatornaszámot kell megadni; a *–w* kapcsoló után a fájlnevet, melybe rögzíteni kívánjuk a csomagokat; a *–b* kapcsoló után pedig a BSSID oszlopból kimásolt (AP) MAC-címet kell megadni.
5. A következőkben két lehetőségünk van: vagy várunk, hogy megfelelő mennyiségű csomagot fogjunk el a hálózatban vagy mi magunk generálunk hálózati forgalmat. Ez utóbbihoz nyújt segítséget az *aireplay-ng* program, mely csomagokat injektál a hálózatba. A következő parancs kiadásával hamis hitelesítési csomagokat küldünk a hozzáférési pontnak így készítve elő az ARP visszajátszásos támadást (ARP-replay):
   aireplay-ng -1 0 -a AP_MAC_ADDR -h FAKE_MAC_ADDR -e SSID eth1
   A kapcsolók között a *-1* a hitelesítési támadásra utal; a *0* az újrakapcsolódási időköz másodpercben megadva; a *–a* kapcsolónál az AP MAC-címét kell megadni; a *–h* kapcsolónál megadhatjuk, hogy milyen hamis MAC-címről érkezzenek a hitelesítési kérelmek; végül a *–e* kapcsolóval az AP által hirdetett SSID nevét kell megadni.
6. A következő lépésben az általában jól megbízható ARP visszajátszásos támadással generálunk új, IV-t tartalmazó csomagokat. A támadás során a program mindig ugyanazt az ARP csomagot küldi vissza az AP-nak, ami mindig új IV-vel küldi vissza a csomagot. A következő parancs végrehajtásával tudunk ARP visszajátszást végrehajtani: *aireplay-ng -3 -b AP_MAC_ADDR -h FAKE_MAC_ADDR eth1*

[41] http://www.aircrack-ng.org/doku.php

A *-3* kapcsoló a támadás típusát határozza meg (ARP-replay); a *–b* az AP MAC-címét; és a *–h* a hamis MAC-címet, ahonnan érkezzenek az ARP-kérések.

7. Utolsó lépésben – miután megfelelő számú csomagot gyűjtöttünk – az aircrack-ng programnak beadjuk a csomagokat tartalmazó fájlt, majd meghatározzuk a WEP-kulcsot a következő parancs kiadásával: *aircrack-ng -n WEP_KEY_LENGHT -b AP_MAC_ADDR CAPFILE_NAME*

   A *–n* kapcsoló után kell megadni a WEP kulcs hosszát bitekben (64, 128); a *–b* kapcsoló után az AP MAC-címét és legutolsó paraméterként a fájl elérési útját kell megadni. Amennyiben a kulcs hosszát nem pontosan adjuk meg, nem fogunk eredményre jutni.

A tesztelés során nem generáltam ARP csomagokat, hanem megvártam, hogy a hálózatban található állomás elegendő csomagot generáljon. Ennek érdekében online videókat néztem, és kb. 10 perc alatt összegyűlt a megfelelő mennyiségű adatcsomag (128 bites WEP-kulcs esetén >80000 csomag). Amennyiben visszajátszásos támadást is alkalmaz a támadó, akkor a WEP kulcs feltöréshez akár 5 perc is elegendő.

A BackTrackben találhatunk grafikus felülettel rendelkező WEP-kulcstörő programot a SpoonWEP személyében. A SpoonWEP egy Java programozási nyelven megírt, egyszerűen használható program, melyben a kulcs megfejtéséhez meg kell adni az AP MAC-címét, a csatorna számát és a támadás típusát. A SpoonWEP az Aireplay-ng programhoz hasonlóan több támadási típust ismer. A program egyik támadási típusa többek között az ARP visszajátszásos támadást. Amennyiben nem tudjuk, hogy hány bites a kulcs, a program végigpróbálja a különböző kulcshosszakra az algoritmust.

A WPA jelszavak megszerzése a hitelesítés során elfogott adatokra épül. A WPA jelszavakat a PSK (pre-shared key) módszert használó hálózatokban lehet feltörni, mert a WPA által használt TKIP ugyan csomagonkénti kulcsot használ, de az inicializálás során (pl. a hitelesítés során) megszerezethetünk olyan adatokat, amit egy szótártámadás keretében kiértékelhetünk. A WPA gyengesége a 4 utas kézfogásban rejlik, mert léteznek olyan algoritmusok, melyek ezt a nyílt szöveget az elsődleges mesterkulccsá (PMK) változtatják. A támadónak csupán egy teljes hitelesítési folyamatot kell rögzítenie. Folyamat rögzítéséhez nagy szerencse kell, de egy deauthentikációs támadás eredményeképpen kikényszeríthetünk egy hitelesítési folyamatot, azonban ehhez legalább egy asszociált kliensnek lennie kell a hálózatban (melyet

az *airodump-ng* megmond). Ha nincs az AP-hoz asszociált állomás, akkor a támadónak nincs szerencséje.[42]

A megfelelő csomagok megszerzése után már csak egy jó szótárra van szükség és egy törőprogramra. Egy igazán jó szótárt összeállítani nagyon nehéz, de vannak az interneten elérhető és megrendelhető szótárak. Az egyik ilyen szótárt egy CD-n kínálják[43], ami egy 500 MB méretű txt fájl, melyben több mint 40 millió szó található. A tesztelés során egy kisebb méretű szótárt töltöttem le és az *aircrack-ng* programot használtam. Az *aircrack-ng* program jelzi, ha a csomagokat tartalmazó fájlban nincsen érdemleges csomag (azaz a 4 utas kézfogás csomagjai). A tesztelés során a támadó gépe egy Core2Duo 2 GHz processzorral rendelkező laptop volt, mely másodpercenként 80 kulcsot tudott megvizsgálni. Ez nem sok tekintve a 40 millió szó vizsgálatához szükséges időt, ami ezzel a sebességgel 139 óra. A tesztkörnyezetben beállított WPA jelszót két óra alatt sem találta meg a szótártámadás segítségével az *aircrack-ng*, ezért terminálatam a programot. Az *aircrack-ng* mellett a BackTrack gyűjteményben megtalálható a népszerű *coWPAtty* jelszótörő alkalmazás is.

6.6. Hálózati eszközök, állomások és szolgáltatások feltérképezése

Miután kapcsolódtunk egy hálózathoz és tudunk adatot forgalmazni, elkezdhetjük a hálózati hierarchia rekonstruálását. Ehhez több, a BackTrack-ben megtalálható program is segítséget nyújt. Az egyik ilyen program az EtterApe, mely vizuálisan megrajzolja az állomások, azok kapcsolatainak és a használt protokollok közötti összefüggéseket. Egy másik program az Angry IP Scanner egy hálózati felderítő program, mely a saját címtartományunkban végignézi a ping parancs segítségével, hogy mely IP-címek vannak használatban. Az Angry IP Scannert be lehet állítani, hogy ne csak az IP-címeket vizsgálja, hanem a nyitott portokat is. A BT-ben megtalálható egy AutoScan Network 1.26 nevű alkalmazás, mely az előbb említett funkciókat szintén ellátja, de ezen felül további információkkal szolgál az állomásokról. Ilyen információ lehet pl.: az operációs rendszer típusa és verziószáma, a processzor típusa, a memória mérete, stb. A grafikus felülettel rendelkező programok mellett a BT-ben találhatunk parancssoros programokat, mint például az *nmap*. Az *nmap* is egy hálózati felderítő program, mely a

[42] http://docs.lucidinteractive.ca/index.php/Cracking_WEP_and_WPA_Wireless_Networks

[43] http://www.openwall.com/wordlists

portokat is vizsgálja[44]. Tervezése során elsődleges szempont volt, hogy gyorsan lehessen nagyméretű hálózatokat vizsgálni vele. Az *nmap* raw IP csomagokat (olyan csomagok, melyek a 4. rétegben még nem lettek feldolgozva)[45] használ annak eldöntésére, hogy mely állomások érhetőek el a hálózatban, azok milyen szolgáltatásokat kínálnak és milyen operációs rendszert futtatnak. Az *nmap* keresést kapcsolók segítségével tudjuk szabályozni.
Azonban nem csak Linux környezetben találhatunk erre a célra fejlesztett programokat. Az egyik általam is kipróbált Windows alapú hálózatfeltérképező program a Fing[46] (elődje a Look@LAN), mely egymagába egyesíti az előbb tárgyalt funkciókat, mindemellett még ingyenes is.
A hálózatban használt szolgáltatásokról átfogó képet kaphatunk a hálózati adatforgalom analizálásával. A Wireshark (régebben Ethereal) egy – a GNU GPL feltételei mellett – ingyenesen használható csomaganalizáló szoftver, melyet hibaelhárításra, analizálásra, kommunikációs protokollok fejlesztésére és oktatásra használnak. A Wireshark számos hálózati rendszer analizálását támogatja, amennyiben az operációs rendszer lehetővé teszi. Például: Ethernet, Token-Ring, FDDI, soros interfész (PPP és SLIP), 802.11 WLAN, ATM.

6.7. Jogosultság szerzése

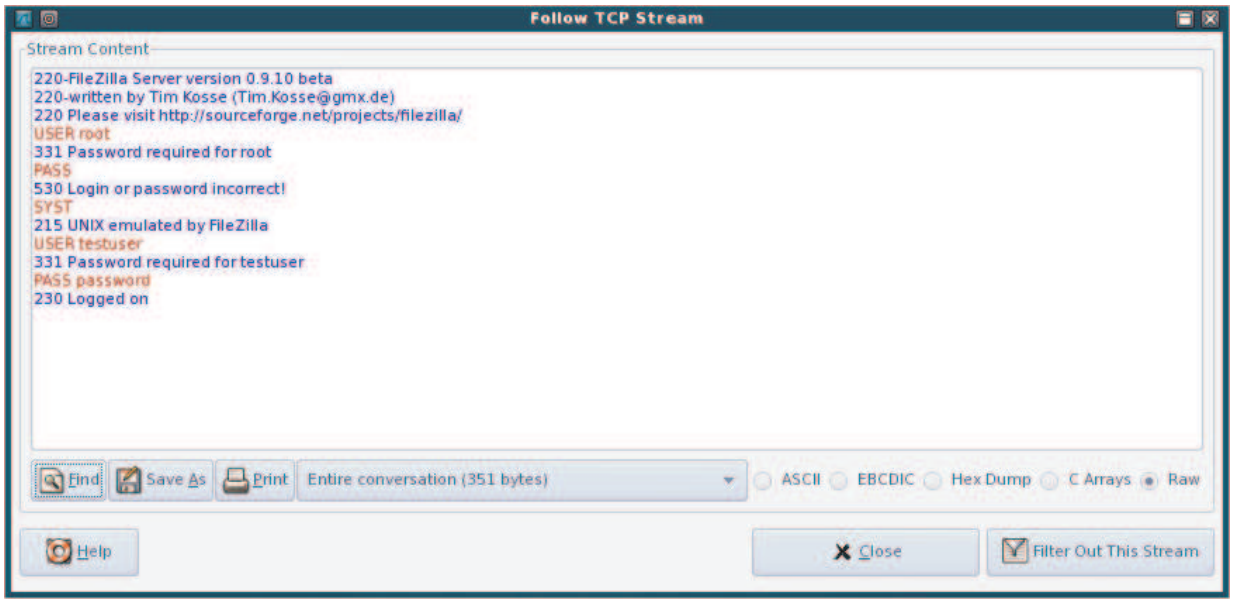
A hálózati eszközök és szolgáltatások felfedezése után a következő lépés a megfelelő jogosultság megszerezése, melynek több módja van. A legkézenfekvőbb a hálózati adatforgalom lehallgatása, majd az ott nyílt üzenetben továbbított jelszavak felhasználása (pl. SNMP, FTP, stb.). Ezen módszert szemléltetve a tesztelés során FTP bejelentkezési információkat fogtam el úgy, hogy az áldozat gépén futó FTP szerverre bejelentkeztem egy tesztfelhasználóval, miközben a hálózatban található csomagokat Wireshark programmal a támadó gépén gyűjtöttem. Az elfogott csomagok alapján rekonstruáltam a TCP adatfolyamot. A Wireshark ezen opciója lehetővé teszi a csatlakozás menetének és a csatlakozás során használt adatok átfogó és szemléletes bemutatását (7. ábra).

---

[44] http://nmap.org/man/hu/

[45] www.linuxvilag.hu/content/files/cikk/16/cikk_16_49_53.pdf; *52.o.*

[46] http://www.over-look.com/site/index.php/documentation/fing-features



7. ábra: TCP adatfolyam végigkövetése Wiresharkban

Egy kisebb hálózatban alkalmazható módszer az is, ha úgy jutunk pl. az AP hozzáférési adataihoz (ezáltal a hálózati forgalom vezérléséhez), hogy a hálózatban található MAC-címek közül egyet kiválasztva a másik állomással egy időben mi is generálunk hálózati forgalmat. Ezt valószínűleg érzékelni fogja a hálózat üzemeltetője is és előbb vagy utóbb ellenőrzi az AP konfigurációját. Ha a konfiguráció ellenőrzésekor sniffer programot futtatunk, jó eséllyel megszerezhetjük az AP hozzáférési adatait. A hálózati adatforgalom figyelésével és különböző jelszavak elfogásával nem csak technikai információt szerezhet egy támadó, hanem olyan információkat is, melyeket később akár egy komolyabb támadás előkészítéséhez is felhasználhat. Például, ha a támadó elfog fontos neveket, címeket tartalmazó beszélgetéseket – legyen akár e-mail vagy egy csevegőprogram által küldött adat – akkor később ezekre személyesen vagy levélben is hivatkozhat.

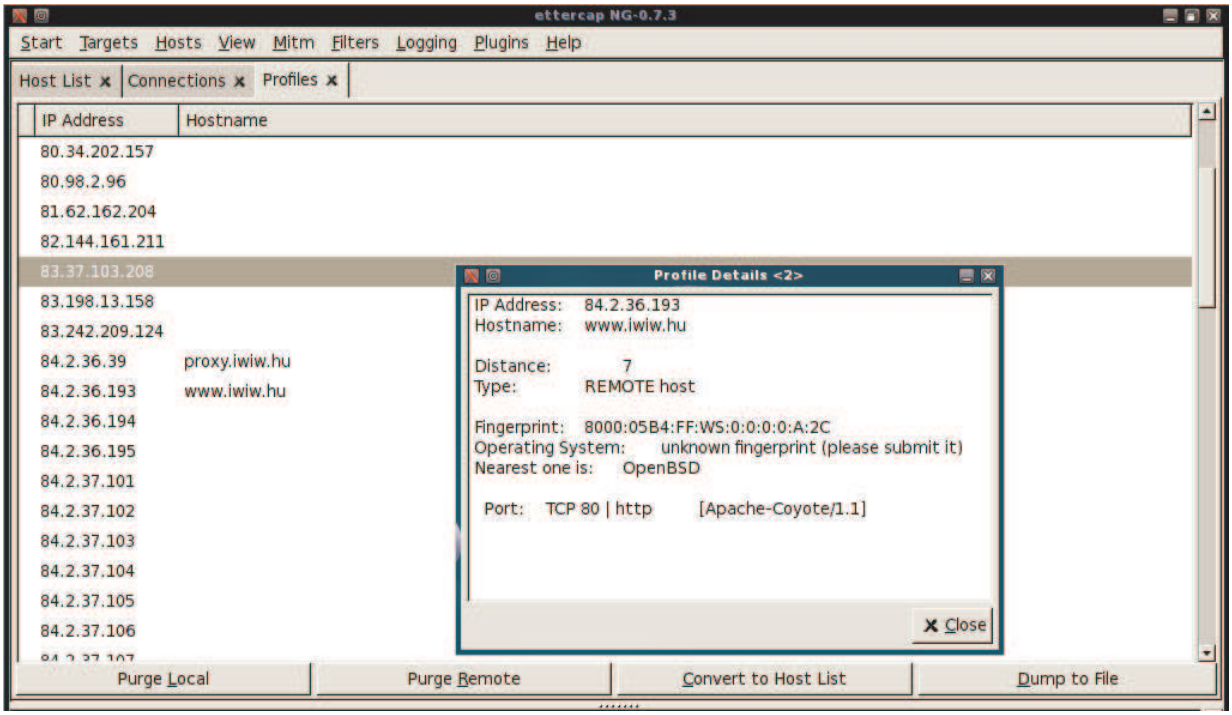
A jogosultság megszerzésének egy kifinomultabb módszere a man-in-the-middle támadás és a rendszerek biztonsági réseinek (privilege escalation) kihasználása. A BT-ben számos program és keretrendszer áll rendelkezésre ezen, komolyabb tudást és jártasságot igénylő programok és keretrendszerek használatához. Man-in-the-middle támadásokat használó program például az eredetileg lehallgató programnak készülő Ettercap NG, ami mára egy sokoldalú sniffer és tartalomszűrő alkalmazássá nőtte ki magát és a man-in-the-middle támadások elengedhetetlen eszközé vált. Többféle protokoll (köztük titkosított protokollok) aktív és passzív lehallgatására alkalmas, továbbá számos hálózat- és állomásanalizáló funkcióval rendelkezik. Az Ettercap a következő funkciókat nyújtja:

- SSH1 felhasználói nevek, jelszavak és adatok lehallgatása SSH1 kapcsolatban.
- SSL-el biztosított adatok lehallgatása hamis tanúsítvány biztosításával.
- Karakterek injektálása meglévő kapcsolatba (pl. szerverparancsokat emulálva)
- Csomagok szűrése/eldobása szűrő-scripteket alapján (pl. bizonyos sztringek keresése TCP vagy UDP csomagokban, ezek cseréje vagy a teljes csomag eldobása)
- Jelszógyűjtés a következő protokollokhoz: telnet, FTP, POP, RLOGIN, SSH1, ICQ, HTTP, SMB, MySQL, IRC, BGP, IMAPv4, LDAP, SNMP, MSN, stb.
- Passzív OS információszerzés (fingerprinting) pl.: operációs rendszer típusa, futó szolgáltatások, nyitott portok, IP és MAC-cím, hálózati kártya gyártója.

Az Ettercapet lehet parancssorból különböző kapcsolók megadásával, illetve grafikus felülettel is használni. Tesztelése során a grafikus felületet használtam. A program indítása után a megfelelő interfészt kiválasztva meg kell keresnünk a hálózatban található állomásokat. Az állomáskeresés eredményeképpen egy listát kapunk a hálózatban található állomásokról, majd ebből a listából kiválaszthatjuk a célpont-állomásokat. A man-in-the-middle támadások esetében, legalább két célpontot kell megadni (két célpont közé ékelődik a támadó, jelen esetben az Ettercapet futtató állomás). A tesztelés során az alapértelmezett átjáró és az áldozat IP-címét adtam meg célpontként. A támadó gépén a lehetséges man-in-the-middle támadási típusok (ARP mérgezés, ICMP átirányítás, port lopás, DHCP hamisítás) közül az ARP mérgezést választottam. A névfeloldásra használt ARP protokoll támadásának lényege, hogy az ARP kérések során a támadó mindig hamarabb válaszol, mint az érintett állomás, így az ARP kérést küldő állomás ARP-táblájában az adott MAC-címen a támadó IP-címe lesz megtalálható. Ha ezt sikerül mind a két félnél elérnie, akkor a két állomás közé ékelődve minden adat a támadón keresztül fog haladni. A *Start sniffing* (lehallgatás indítása) utasítás kiadását követően egy külön ablakban megtekinthetőek az egyes állomásokhoz tartozó kapcsolatok (8. ábra). Ezeket a kapcsolatokat lementhetjük egy fájlba, terminálhatjuk őket, illetve fájlokat és csomagokat injektálhatunk közvetlenül a kapcsolatba.

A tesztelés során az áldozat gépén bejelentkeztem az iWiW közösségi portálra és ezt követően azonnal megjelent az Ettercap programban a bejelentkezési név és jelszó páros, továbbá az, hogy milyen URL címről érkezett az adat. Ezzel jogosultságot szereztem egy, az áldozat által használt szolgáltatáshoz. Az Ettercap, hamis tanúsítvány biztosításával SSL-titkosítást használó oldalak esetében is jól működik. Ezt a Google által kínált Gmail levelező szolgáltatás elindításával teszteltem. Az áldozat gépén az URL beírását követően a böngésző

jelezte, hogy a tanúsítvány nem megfelelő, de miután elfogadtam a tanúsítványt és bejelentkeztem, az Ettercap-ben megjelentek a bejelentkezési adataim. A tanúsítványt megvizsgálva a tartalom nagy része megegyezik az eredeti tanúsítvánnyal, azonban a kiállító ismeretlen (unknown issuer).



8. ábra: Kapcsolatok részleteinek megjelenítése az Ettercap programban

A jogosultság megszerzésének másik módszere a biztonsági réseket kihasználó keretrendszer használata, melyre példa a MetaSploit Framework3. A Framework3 modulárisan van felépítve és az egyes moduljai a különböző biztonsági rések kihasználására vannak megírva. Ilyen modulok pl. a Tomcat webszerver adminisztrációs felületét feltörő; Oracle adatbázisokhoz hozzáférést szerző; különböző FTP szerverek elleni támadás és hozzáférést szerző modulok, stb.[47]

A különböző szolgáltatások, alkalmazások és operációs rendszerek hibáinak kihasználására nem térek ki a dolgozat témája miatt.

[47] http://www.metasploit.com/framework/modules/

7. Szimulálás eredményének értékelése

A tesztelés és a kutatás során számos biztonsági problémába futottam bele, melyek egy része az IEEE 802.11 protokoll tervezési hibáiból adódott, míg más problémákat felhasználói és hálózatüzemeltetési okokra lehet visszavezetni. A kérdés, miszerint létezik-e biztonságos vezeték nélküli hálózat jogosan merül fel. A válasz megtalálásához és a megfelelő indokláshoz azonban több tényezőt figyelembe kell venni. A kérdés vizsgálata során különbséget kell tenni a vállalati szintű és az otthoni/kis- és középvállalatok által használt technológiák között. [48]

A nagyfokú marketingnek köszönhetően, amely a vezeték nélküli hálózatok kétségtelen előnyeit hangsúlyozza – pl. rugalmasság, mobilitás, vezetékek felszámolás – a biztonságról sokszor elfeledkeznek. A másik oldalról azonban néhány vállalat a nem megfelelő informáltság és tudatlanság következtében tiltja a vezeték nélküli technológia használatát. A vezeték nélküli hálózatokat ugyanúgy meg kell tervezni, mint a vezetékes hálózatokat. A vezeték nélküli hálózatokat fenyegető támadások nagy része elkerülhető lenne megfelelő tervezés mellett, azonban be kell látnunk, hogy teljesen biztonságos hálózat nincsen – sem vezetékes, sem vezeték nélküli.

A vezeték nélküli hálózatok előnye, hogy nem kell vezetékekkel bajlódni, viszont ebből következik az a jellegzetességük is, hogy nem az épület falai szabják meg a hálózat határát. A WLAN tervezésekor tudatosan figyelni kell a lefedettségre és kerülendő eljárás az, hogy két-három épülettel arrébb is látható és támadható a hálózat. (Gast [2005]) Az ilyen problémákat SOHO (Small Office/Home Office - kis vállalatok és otthoni) hálózatok esetén az AP megfelelő beállításával lehet korrigálni (adó teljesítményét csökkentjük). Vállalati környezetben azonban egy menedzsment rendszer szükséges (pl. Cisco WCS; Aruba ARM – automatikus RF menedzsment), mely többek közt szabályozza a hálózat kiterjedését és lefedettségét[52]. Egy megfelelő hálózatmenedzsment alkalmazásnak feladata, hogy monitorozza a hálózatot és figyelje az illetéktelen felhasználókat, illetve az idegen (rouge) hozzáférési pontokat. Az idegen AP-k veszélyeiről az 5. fejezetben írtam. Joshua Wright, *www.willhackforsushi.com* oldal kitalálója egy interjú során azt nyilatkozta, hogy egy kórház biztonsági tesztelése során hónapokig volt egy idegen AP a kórház hálózatában, miután gyomorfájást színlelve egy folyósón elhelyezte a saját eszközét. Az eszköz pár hónap után

[48] http://www.hwsw.hu/hirek/43067/aruba-networks-vallalati-wi-fi-802-11n-halozat-biztonsag.html

abbahagyta az adást. Amikor Wright bement elkérni a biztonsági őröktől a megtalált eszközt, szembesülnie kellett azzal, hogy nem a biztonságiak találták meg, hanem ellopták.[49]

A WLAN tervezése során gondolni kell arra, hogy a levegőben továbbított adatcsomagokat bárki láthatja, ezért azokat titkosítani kell. A dolgozat során megvizsgáltam a különböző titkosítási protokollokat és megállapítottam, hogy ma a WPA2 szabvány által kínált megoldás teljesen biztonságos, míg a WPA szabvány esetében bizonyos megszorítások kell alkalmazni (például erős, legalább 8 karakter hosszúságú jelszó használata, mely nem kombinálható ki szótári szavak alapján). A tesztelés során kiderült, hogy egy gyenge titkosítást (WEP) alkalmazó hálózathoz egy 5 perces jelszótörési folyamatot követően már csatlakozni lehet. A lehallgatást, a csomaginjektálást és a csomagvisszajátszás lehetőségét a vállalati WLAN esetében a 802.11i szabvány RSN protokolljainak alkalmazásával lehet csökkenteni.[50] Itt kapcsolódik a vezeték nélküli hálózatokhoz a hitelesítés és jogosultság kezelésének kérdése. A hitelesítés során meghatározzuk, hogy ki férhet hozzá a hálózati erőforrásokhoz. Egy nyílt hitelesítést alkalmazó vezeték nélküli hálózathoz bárki hozzáférhet, amennyiben tudja a hálózat SSID-ját és a titkosítás során alkalmazott kulcsot (amennyiben van titkosítás beállítva). A MAC-címszűrés sem a leghatékonyabb módja a hitelesítésnek, hiszen elég sebezhető. A hitelesítés és jogosultságok kezeléséhez a nagyvállalatok a 802.1x keretrendszert használhatják. A 802.1x szabvány alkalmazása során fontos, hogy a vállalat a megfelelő EAP protokoll használata mellett döntsön. Amennyiben egy kevésbé biztonságos EAP protokollt választanak a tervezés és implementáció során, úgy könnyen fontos információk kerülhetnek a támadó birtokába. Például ha a PEAP protokoll ellen sikeres támadást hajt végre egy támadó, akkor akár Windows tartományi felhasználó nevet és jelszót szerezhet, ezáltal pedig további szolgáltatásokat vehet igénybe és támadhat meg. A 802.1x szabvány alkalmazásakor telepíteni kell egy RADIUS szervert is. Ez otthoni felhasználás esetében általában nem kifizetődő és az ilyen szintű biztonság sokszor indokolatlan is. Azonban a kis- és az ezektől nagyobb vállalatok esetén ez a megfelelő biztonság érdekében elhagyhatatlan. A különböző EAP protokollok különböző lehetőségeket kínálnak. Például egyes EAP protokollok lehetővé teszik a biometrikus azonosítás alkalmazását.

A 802.1x rendszer egy második rétegbeli védelmet nyújt. Azonban a vezeték nélküli hálózatokat is védeni kell az első réteg szintjén. A fizikai védelembe beletartozhat az AP és a

[49] http://blogs.techrepublic.com.com/wireless/?p=205

[50] http://www.networkworld.com/community/print/19898

hálózati eszközök megfelelő elhelyezése (pl.: az AP-t nem az asztalra kell helyezni, hanem megfelelő magasságba kell felszerelni), a hálózati eszközöket tartalmazó helyiség megfelelő védelme (az ott tárolt eszközök értékének és stratégia fontosságának megfelelően). A fizikai védelemhez hozzátartozhat, hogy idegen nem tartózkodhatnak egyedül a vállalat területén, illetve a személyazonosságukat hitelesen igazolni kell a belépéskor.

A fizikai védelemhez kapcsolódik az átviteli közeg biztosítása. Azon vállalatok, melyek értékes információkat továbbítanak vezeték nélküli hálózaton, szükségük van az átviteli közeg állandó figyelésére, monitorozására és a rádióadás szabályozására. Egy vállalati WLAN rendszerben nyomon kell tudni követni az állomások aktivitását, egy külső vagy belső állomás forgalmában bekövetkezett változást, ami utalhat egy DoS vagy egy man-in-the-middle támadásra.[51] Ezen problémák egy része megfelelő tervezéssel megelőzhető, azonban szükség van valós idejű megfigyelésre, valamilyen monitor tevékenységre (pl. az idegen AP detektálásához, helyzetük meghatározásához). A hálózati átviteli közeg figyelését számos eszköz segíti: idegen eszközöket felderítő kézi eszközök; vezeték nélküli IDS/IPS, mely lehetővé teszi a valós idejű hálózati forgalomanalizálást és probléma esetén megfelelő lépéseket tud tenni (IDS esetében lehet ez riasztás, IPS esetében pedig az adott kapcsolat bontása); vezeték nélküli spektrum analizátor, mellyel a RF interferenciát lehet kiszűrni.

A vezeték nélküli hálózatok biztonsága függ a hálózatban található állomások helyi szintű szabályozásától, védelmétől. Az állomásokat kliens oldali tűzfallal, kliensre telepített IDS/IPS rendszerrel, vírusirtó alkalmazással, különböző központilag vezérelt házirend betartatásával (pl. jelszóházirend szabályozza a felhasználói jelszavak formáját és megváltoztatásának gyakoriságát) kell védeni. Nagyon fontos és sok helyen háttérbe kerülő szempont az egyes állomások hálózati kártyájának meghajtó-programja (driver).[52] Az egyes eszközökhöz írt meghajtó-programok a kiadáskor messze nem tökéletesek és biztonsági réseket tartalmaz(hat)nak. Ezen okokból kifolyólag az állomásokban található kártyának mindig a legújabb meghajtó-programot kell használnia. A jelszavakat nem csak az állomásokon kell megfelelően megválasztani, hanem a hálózati eszközökön is (AP, kapcsoló, stb.). Például egy alapértelmezett SSID-t hirdető AP-hoz tartozó bejelentkezési adatok (felhasználói név/jelszó) nagy valószínűséggel a gyári alapadatok, mert aki üzembe helyezte az eszközt valószínű,

[51] http://www.networkworld.com/community/print/19898

[52] http://blogs.techrepublic.com.com/wireless/?p=205

hogy nem állította át ezeket az adatokat, ha az SSID-t sem változtatta meg.[53] Sok fórumon lehet olvasni, hogy az SSID-t nem szabad hirdetni, azonban itt megoszlik a biztonságtechnikai szakemberek véleménye. Joshua Wright szerint nem szabad megakadályozni az SSID hirdetését, mert adódhat olyan helyzet, amiben pontosan az ellenkezőjét érjük el. Erre hozta azt a példát, hogy ha egy állomás csatlakozni akar egy rejtett SSID-jű hálózathoz, ahhoz végig kell kérdezni az összes AP-t, hogy megtudja a keresett AP adatait. Azonban ha egy hacker meghamisítja ezt az SSID-t, akkor az adott állomás hozzá fog csatlakozni és neki fogja elküldeni a titkos és bizalmas adatokat.[54]

Legutolsó – és sokszor legkomolyabb – biztonsági faktornak a hálózatok szolgáltatásait igénybe vevő felhasználókat említeném (User)[55]. A vezeték nélküli technológiát mindennap használó felhasználók a technológia mélyebb ismerete nélkül sokszor nem figyelnek az alapvető biztonsági szabályzatok betartására, sőt szándékosan megszegik a központi házirendet, anélkül, hogy tudnák mi lehet a következménye. Pl. egy „okos" felhasználó egy otthonról hozott hozzáférési ponttal szeretné rugalmasabbá tenni a munkáját, mely által hatalmas biztonsági rést hozhat létre (a legtöbb esetben létre is hozza). Ez a felhasználó által beüzemelt AP megfelel az idegen (rouge) AP fogalmának, annak ellenére, hogy nem ártó és támadó szándék vezérelte a cselekedete során. Az így elhelyezett eszközöket általában nem vagy csak minimálisan konfigurálják, így kiváló pontja lehet a hálózati behatolásnak. (Thomas [2005]) A felhasználó az a biztonsági tényező, aki gyenge jelszavakat használ (amennyiben nem követeli meg házirend az erős jelszó használatát), mint például a kutyája nevét adja meg bejelentkezési jelszóként – melyet felír egy cetlire – és kiragasztja a monitorára, hogy ne felejtse el. A felhasználók sokszor adnak ki illetékteleneknek információkat és könnyű őket becsapni. Ha egy támadó előzetesen felméri (pl. személyesen) a célhálózatot és megvizsgálja annak felhasználóit, egy körképet kaphat a biztonság mértékéről. A felhasználók azok, akik sokszor letiltják a vírusirtót, mert „nagyon belassítja a számítógépet" és ezzel újabb biztonsági rést hagynak a támadónak. Előszeretettel osztanak meg dokumentumokat, melyek hozzáférési jogait nem állítják be, így egy hálózat feltérképezése során a támadó rögtön láthatja a megosztott meghajtókat, mappákat, állományokat. A felhasználók hajlamosak mindenre OK-t nyomni, hogy bejöjjön az általuk

[53] http://www.wi-fiplanet.com/tutorials/article.php/3605601

[54] http://blogs.techrepublic.com.com/wireless/?p=205

[55] http://iesb.hu/human-biztonsag/leggyengebblancszemember/

óhajtott honlap, így fogadva el hamis tanúsítványt pl. egy man-in-the-middle támadás során. Komoly problémát jelentenek a belső támadók, akik a hálózatban felhasználó szerepet töltenek be és valamilyen szinten ismerik a hálózat felépítését. Az ilyen módon elkövetett támadásokat rendszeres monitorozással, naplózással és ACL használatával lehet szabályozni. A felhasználók miatti biztonsági rést lehet szűkíteni (véleményem szerint teljesen nem lehet megszüntetni) ha rendszeres oktatásban részesülnek, külön felhívják a figyelmüket az egyes veszélyforrásokra és nyomtatékosan betartatják velük a házirendet. Minden szabály csak akkor ér valamit, ha betartják, illetve betartatják. Ez különösen igaz a hálózati biztonság területén.

A dolgozatírás során számos tapasztalatot szereztem és ezek egyikét most részletesen leírom, mert tanulságos. Az egyik tesztelési helyszíntől nem messze található egy gyógyszertár, melyben egy WLAN üzemel, ami kb. 70-80 m távolságra is látható. A patika WLAN hálózatának SSID-ja a patika neve, így bárki könnyen be tudja azonosítani a hálózatot. A hálózatban nyílt hitelesítés van (MAC-címszűrés nincs) és semmilyen titkosítás nincs beállítva. A hálózathoz csatlakozva egy DHCP kiszolgálótól (az AP) rögtön IP-címet lehet kapni a 192.168.2.0/24 hálózatból. Az IP-címmel együtt átadja a DNS kiszolgáló és az alapértelmezett átjáró IP-címét, ami 192.168.2.1 IP-című AP. Az alapértelmezett átjáró IP-címét a böngészőbe beírva rögtön az AP beállítási oldala jön be, ahol az alapértelmezett adminisztrátori jelszóval rögtön be is lehet lépni az AP konfigurációs oldalára. Ha egy képzeletbeli támadó egy hálózat feltérképezést tartana, akkor látná, hogy a hálózatban kettő állomás (két kassza) és egy Windows Server 2003 hálózati operációs rendszert futtató szerver található. A hálózati feltérképezés után kiderülne, hogy az egyik állomáson a távoli asztal eléréséhez szükséges port nyitott, így arra rákapcsolódva máris egy bejelentkező felület jelenne meg, ami (akár) közvetlen hozzáférést biztosíthat a jelszó és felhasználói név ismeretében a patika és a vevők adataihoz (nem beszélve a készletről). A képzeletbeli támadó akár egy DoS támadást is indíthatna a hálózati középpontjában található AP ellen, így bénítva meg a patika működését, de akár komplexebb támadást is végrehajthatna. Könnyen elképzelhető, hogy egy-két napos forgalomgyűjtés után a támadó értékes jelszavakat foghatna el. A támadó lehetőségei szinte korlátlanok egy ilyen hálózatban és határt csak a tudása és türelme szabhat (ha már a hálózatot beállító személy nem szabott neki).

De mit mulasztottak el a WLAN beállításánál és hogyan lehetne biztonságossá tenni a hálózatukat? Az alábbiakban felsorolom, mely biztonsági beállítások megtétele lenne szükséges egy ilyen – tipikusan nem nagyvállalati – hálózat esetében:

- Rádióadó teljesítményének csökkentése (így nem látszódna 80 m távolságra a WLAN)
- SSID szórásának tiltása
- MAC-címszűrés használata
- Erős titkosítás használata (legalább WPA2 AES, de ha WPA PSK akkor is 10 karakternél hosszabb, erős jelszó)
- DHCP tiltása, IP-címek manuális kiosztása (3 cím esetén egyáltalán nem megterhelő)
- AP alapértelmezett jelszavának megváltoztatása erős jelszóra
- A hozzáférési ponton engedélyezni kell a tűzfal funkciót, és ha lehetséges, akkor HTTPS-t kell használni
- Naplózás bekapcsolása
- Nem használt portok és protokollok tiltása
- Megosztás kikapcsolása
- Tűzfalak használata a klienseken

A felmerülő kérdésre végső konklúzióként megállapíthatjuk, hogy létezik biztonságos vezeték nélküli hálózat, azonban számos tényezőt kell figyelembe venni:

- az implementációt alapos tervezésnek kell megelőznie, mely során sok sebezhetőséget kizárhatunk
- az implementáció során be kell tartani bizonyos biztonsági útmutatásokat és törekedni kell a maximális védelemre, továbbá a költségvetésnek nem szabad a biztonság rovására mennie
- a hálózat kiépítése után jelentkező menedzsment feladatokat el kell látni és bizonyos időközönként hálózati monitorozást kell végrehajtani
- a felhasználókat tájékoztatni kell a veszélyforrásokról, éberségüket fenn kell tartani
- megfelelő biztonsági házirenddel kell rendelkeznie egy hálózatnak, melyben rögzítve vannak a következők: hatályosság, általános szabályok, biztonsági és tulajdonjogi információk, jelszóvédelmi szabályok, büntetések

Összefoglalás

A vezeték nélküli hálózatok biztonsága aktuális probléma a hálózatok világában. Dolgozatom során a biztonságos vezeték nélküli hálózat megvalósításának feltételeit és folyamatát vizsgáltam meg.

A vizsgálat során bemutattam ezt a nem sokkal több, mint 10 éves technológia elméleti hátterét, a hálózatot alkotó eszközöket és azok funkcióit. A jelenleg elérhető hálózati megoldások közül ismertettem a 802.1x szabványon és a RADIUS protokollon nyugvó vállalati biztonsági megoldást.

A vezeték nélküli hálózatok esetében az egyszerű hozzáférés miatt kiemelt jelentősége van a hitelesítésnek és a hozzáférés-vezérlésnek. A dolgozatban kifejtettem a vezeték nélküli hálózatokban használt hitelesítési metódusokat (nyílt hitelesítés, MAC-cím alapú hitelesítés, osztott kulcsú hitelesítés) és az elmúlt 10 év során kifejlesztett titkosítási protokollokat, szabványokat (WEP, WPA, WPA2, 802.11i).

Biztonságos vezeték nélküli hálózatot csak akkor lehet építeni és működtetni, ha ismerjük a hálózatot fenyegető veszélyeket. A támadási módszerek ismertetésekor a támadó motivációját és célját előtérbe helyezve bemutattam a különböző támadási típusokat.

Az elméleti ismeretek mellett a dolgozatomban a vezeték nélküli hálózatok biztonsági kérdéseit a gyakorlati oldalról is megközelítettem. A munka során számos szoftverrel megismerkedtem. A kialakított laborhálózat lehetőséget nyújtott az elméleti tárgyalás során bemutatott támadások gyakorlatban való alkalmazására, így tudtam például tesztelni a WEP titkosítás gyengeségét és a man-in-the-middle támadás hatékonyságát.

A laborhálózatban végzett tesztelésekre támaszkodva megállapítottam a biztonságos vezeték nélküli hálózatok feltételeit és egy példára támaszkodva rávilágítottam, hogy milyen lépéseket kell(ene) megtenni a biztonság érdekében.

A dolgozat megírásakor sok témakört csak érintettem, mert mind a hálózatok témaköre, mind pedig a hálózati biztonság – azon belül is a vezeték nélküli hálózatok biztonsága – hatalmas terület. Munkámmal igyekeztem rávilágítani a biztonság fontosságára és összegezni azokat a tapasztalatokat, amelyek útmutatásul szolgálhatnak egy biztonságosabb vezeték nélküli hálózat kialakításánál.

Irodalomjegyzék

Felhasznált könyvek:

[1] Beaver, K – Davis, P. T. (2005): Hacking Wireless Networks For Dummies®. Wiley Publishing, Inc., USA

[2] Carroll, B. C. (2009): CCNA Wireless Official Exam Certification Guide. Cisco Press, USA

[3] Certified Wireless Network Administrator Official Study Guide (2002). Planet 3 Wireless, USA

[4] Flickenger, R. (2003): Wireless Hacks. O'Reilly, USA

[5] Gast, M. (2005): 802.11® Wireless Networks The Definitive Guide. O'Reilly, USA

[6] Geier, Jim (2005): Vezeték nélküli hálózatok. Panem Könyvkiadó, Budapest

[7] Geier, Jim (2005): Wireless Networks First-step. Cisco Press, USA

[8] Hucaby, D. (2007): CCNP Self-Study: CCNP BCMSN Official Exam Certification Guide, Fourth Edition. Cisco Press, USA

[9] Nichols, R. K. – Lekkas, P. C. (2002): Wireless Security Models, Threats, and Solutions. McGraw-Hill Companies, Inc., USA

[10] Roshan, P. – Leary, J. (2003): 802.11 Wireless LAN Fundamentals. Cisco Press, USA

[11] Sankar, K. – Sundaralingam, S. – Miller D. – Balinsky, A. (2004): Cisco Wireless LAN Security. Cisco Press, USA

[12] Thomas, Tom (2005): Hálózati biztonság. Panem könyvkiadó, Budapest

[13] Velte, T. J. – Velte, A. T. (2005): Cisco 802.11 Wireless Networking Quick Reference. Cisco Press, USA

Cikkek:

[1] Buttyán L. – Dóra L. (2006): WiFi biztonság – A jó, a rossz és a csúf. Hírközlési és Informatikai Tudományos Egyesület folyóirata, LXI. ÉVFOLYAM 2006/5

Internetes források:

[1] BCS Hungary: Wi-Fi hálózatok menedzsmentje. Letöltve: 2009.11.07-én a következő oldalról: www.bcs.hu/letoltes.php?d_id=823

[2] Buttyán Levente és Dóra László (2006): WiFi biztonság – A jó, a rossz, és a csúf. Letöltve: 2009.10.19-én a következő oldalról: http://www.crysys.hu/publications/files/ButtyanD06ht.pdf

[3] Cam-Winget, N. – Moore, T. – Stanley, D. – Walker, J. (2002): IEEE 802.11i Overview. Letöltve: 2009.10.27-én a következő oldalról: http://csrc.nist.gov/archive/wireless/S10_802.11i%20Overview-jw1.pdf

[4] Cisco Wireless Control System Configuration Guide. Letöltve: 2009.10.18-án a következő oldalról: http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcsmaps.pdf

[5] Cisco Wireless Control System (WCS). Letöltve: 2009.11.05-én a következő oldalról: http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html

[6] CrySys Adatbiztonság Laboratórium (2007): Mérési útmutató a „Hálózati protokollok vizsgálata lehallgatással (HIT1)” című méréshez. BME, Letöltve: 2009.10.14-én a következő oldalról: http://www.crysys.hu/infsec/sniff-meres.pdf

[7] Dajkó Pál (2009): Véglegesítették a 802.11n szabványt. Letöltve: 2009.10.02-én a következő oldalról: http://itcafe.hu/hir/wifi_szabvany.html

[8] Faigl László Az IEEE 802.11i kapcsolat-felépítés vizsgálata – RADIUS alapú hitelesítés EAP-TLS módszerrel WLAN hálózatban. Letöltve: 2009.10.11-én a következő oldalról: http://kutfo.hit.bme.hu/oktatas/802.11i_meres

[9] Fing features. Letöltve: 2009.10.27-én a következő oldalról: http://www.over-look.com/site/index.php/documentation/fing-features

[10] Geier, E. (2006): Wi-Fi Security Issues Up Close. Letöltve: 2009.10.27-én a következő oldalról: http://www.wi-fiplanet.com/tutorials/article.php/3605601

[11] Griffith, E. (2004): 802.11i Security Specification Finalized. Letöltve: 2009.10.10-én a következő oldalról: http://www.wi-fiplanet.com/news/article.php/3373441

[12] hamWiki (2008): Iránykarakterisztika. Letöltve: 2009.09.30-án a következő oldalról: http://wiki.ham.hu/index.php/Ir%C3%A1nykarakterisztika

[13] Index.hu (2009): Egy perc alatt feltörhető a wifi. Letöltve: 2009.10.11-én a következő oldalról: http://index.hu/tech/2009/08/28/egy_perc_alatt_feltorheto_a_wifi/

[14] Index.hu (2009): Negyvenéves az internet. Letöltve: 2009.09.10-én a következő oldalról http://index.hu/tech/2009/09/02/negyven_eves_az_internet/

[15] Információ és biztonság (online folyóirat): A leggyengébb láncszem: az ember. Letöltve: 2009.10.02-én a következő oldalról: http://iesb.hu/human-biztonsag/leggyengebblancszemember/

[16] Információ és biztonság (online folyóirat): A WEP protokoll. Letöltve: 2009.10.02-én a következő oldalról: http://iesb.hu/logikai-biztonsag/a-wep-protokoll/

[17] Insolvibile, G. (2002): A Linux-csomagszűrő felépítése. Letöltve: 2009.10.27-én a következő oldalról: www.linuxvilag.hu/content/files/cikk/16/cikk_16_49_53.pdf

[18] Kassner, M. (2008): Wi-Fi Security is always one step behind. Letöltve: 2009.10.27-én a következő oldalról: http://blogs.techrepublic.com.com/wireless/?p=205

[19] Kershaw, M. (2009): Kismet Readme. Letöltve: 2009.10.27-én a következő oldalról: http://www.kismetwireless.net/documentation.shtml

[20] Kocsis Tamás (2009): Mitől más a vállalati Wi-Fi? Letöltve: 2009.10.27-én a következő oldalról: http://www.hwsw.hu/hirek/43067/aruba-networks-vallalati-wi-fi-802-11n-halozat-biztonsag.html

[21] Kommunikálunk. Letöltve: 2009.10.14-én a következő oldalról http://www.borsod-kozoktatas.hu/egyebinfo/diak_web/tudo/kommu.html

[22] Microsoft TechNet (2009): A RADIUS protokoll és összetevői. Letöltve: 2009.10.07-én a következő oldalról: http://technet.microsoft.com/hu-hu/library/cc726017(WS.10).aspx

[23] Microsoft TechNet (2009): A PEAP protokoll – áttekintés. Letöltve: 2009.10.24-én a következő oldalról: http://technet.microsoft.com/hu-hu/library/cc754179(WS.10).aspx

[24] Műszaki lexikon (2008): Elhalkulásmentes (diversity) antenna. Letöltve: 2009.09.20-án a következő oldalról: http://www.volkswagen.hu/volkswagen_koeruel/innovacio/m_szaki_lexikon/diversity_antennen.html

[25] Metasploit Module Browser. Letöltve: 2009.10.27-én a következő oldalról: http://www.metasploit.com/framework/modules/

[26] Montoro, M. (2009): WEP Cracker. Letöltve: 2009.10.01-én a következő oldalról: http://www.oxid.it/ca_um/topics/wep_cracker.htm

[27] Nagy Lajos (1996): Az antennákkal kapcsolatos fontosabb fogalmak és jellemzők. Letöltve: 2009.10.17-én a következő oldalról: http://alpha.tmit.bme.hu/pub/jegyzet/radio.kom/new/anthull4.doc

[28] Németh Árpád Dávid (2005): Social Engineering. Letöltve: 2009.10.27-én a következő oldalról: http://www.securifocus.com/portal.php?pagename=hir_reszlet&hir_id=959&i=

[29] [origo] techbázis (2007): Magyarországon lopás a wardriving. Letöltve: 2009.10.19-én a következő oldalról: http://www.origo.hu/techbazis/internet/20071129-a-szabad-wifihasznalat-lopasnak-minosul.html

[30] Network World (2007): Wireless LAN Security. Letöltve: 2009.10.27-én a következő oldalról: http://www.networkworld.com/community/print/19898

[31] Nmap Referencia Útmutató (Kézikönyv) (2009). Letöltve: 2009.10.27-én a következő oldalról: http://nmap.org/man/hu/

[32] Openwall wordlists collection. Letöltve: 2009.10.27-én a következő oldalról: http://www.openwall.com/wordlists

[33] Orosz P. – Sztrik J. – Soong K. C. (2005): Központosított EAP alapú hitelesítés vezeték nélkül hálózatokban. Informatika a felsőoktatásban 2005 konferencia. Letöltve: 2009.10.10-én a következő oldalról: http://irh.inf.unideb.hu/user/jsztrik/publications/papers/OroszSztrikC14.pdf

[34] Peikari, C. – Fogie, S. (2003): Cracking WEP. Letöltve: 2009.10.21-én a következő oldalról: http://www.airscanner.com/pubs/wep.pdf

[35] Phifer. L. (2003): Using RADIUS For WLAN Authentication, Part I. Letöltve: 2009.10.01-én a következő oldalról: http://www.wi-fiplanet.com/tutorials/article.php/3114511

[36] Phifer. L. (2003): Using RADIUS For WLAN Authentication, Part II. Letöltve: 2009.10.04-én a következő oldalról: http://www.wi-fiplanet.com/tutorials/article.php/3287481

[37] Radiation patterns. Letöltve: 2009.10.15-én a következő oldalról: http://www.tscm.com/radiapat.pdf

[38] Rite, B. (2005): Cracking WEP and WPA Wireless Networks. Letöltve: 2009.10.24-én a következő oldalról: http://docs.lucidinteractive.ca/index.php/Cracking_WEP_and_WPA_Wireless_Networks

[39] RFC 3748 – EAP. Letöltve: 2009. 10.02-án a következő oldalról: http://www.rfc-archive.org/getrfc.php?rfc=3748

[40] RFC 2865 – RADIUS. Letöltve a 2009.10.05-én következő oldalról: ftp://ftp.rfc-editor.org/in-notes/rfc2865.txt

[41] Sankar, K. – Sundaralingam, S. – Miller D. – Balinsky, A. (2004): Cisco Wireless LAN Security. Letöltve: 2009.10.11-én a következő oldalról: http://ciscobook.org.ua/cisco_wireless_lan_security/ch08lev1sec2.html

[42] Secron (2008): Rádiótechnikai ismeretek. Letöltve: 2009.10.12-én a következő oldalról: http://www.secron.hu/Rádiótechnika.html

[43] Schubert, T. (2008): Hálózati szolgáltatások tervezése és működtetése, Vezeték nélküli helyi hálózatok WirelessLAN (WLAN). Letöltve: 2009.11.10-én a következő oldalról: http://nik.bmf.hu/schubert.tamas/H%e1l%f3zati%20szolg%e1ltat%e1sok%20tervez%e9se%20%e9s%20m%fbk%f6dtet%e9se/WLAN%20MSc-2008.pdf

[44] Snyder, J. (2002): What is 802.1x? Letöltve: 2009.10.10-én a következő oldalról: http://www.networkworld.com/research/2002/0506whatisit.html

[45] Tews, E. – Weinmann, R-P. – Pyshkin, A. (2007): Breaking 104 bit WEP in less than 60 seconds. Letöltve: 2009.10.22-én a következő oldalról: http://eprint.iacr.org/2007/120.pdf

[46] Tomcsányi Domonkos és Fóti Marcell (2008): Amit a WPA-törésről tudni kell. Letöltve: 2009.10.10-én a következő oldalról: http://ethicalhacking.hu/wpa.aspx

[47] Tourrilhes, J. (2004): The Linux Wireless LAN Howto. Letöltve: 2009.10.06-án a következő oldalról: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.std.html

[48] Vezetéknélküli lokális hálózatok. Letöltve: 2009.10.11-én a következő oldalról: http://alpha.tmit.bme.hu/meresek/wlan.htm

[49] Wireless Security Tools. Letöltve: 2009.10.27-én a következő oldalról: http://www.corecom.com/html/wlan_tools.html

[50] Wireshark Frequently Asked Questions. Letöltve: 2009.10.27-én a következő oldalról: http://www.wireshark.org/faq.html

Cisco termékek adatlapjai:

[1] Aironet 1130AG
http://cisco.com/en/US/prod/collateral/wireless/ps5678/ps6087/product_data_sheet0900aecd801b901c.html

[2] Aironet 1230AG
http://cisco.com/en/US/prod/collateral/wireless/ps5678/ps6108/product_data_sheet0900aecd801b9266.html

[3] Aironet 1250
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/ps8382/product_data_sheet0900aecd806b7c5c.html

[4] Cisco 1000 Series Lightweight
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6306/ps6315/product_data_sheet0900aecd8025708a_ps6306_Products_Data_Sheet.html

[5] Cisco Aironet 802.11a/b/g Wireless CardBus Adapter:
http://www.cisco.com/en/US/prod/collateral/wireless/ps6442/ps4555/ps5818/product_data_sheet09186a00801ebc29.html

[6] Cisco Aironet 802.11A/B/G Wireless PCI Adapter
http://www.cisco.com/en/US/prod/collateral/wireless/ps6442/ps4555/ps5819/product_data_sheet09186a00801ebc33.html

[7] Cisco 3200 Series Rugged Integrated Services Routers
http://www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheets_list.html

[8] Cisco Aironet 1300 Series
http://www.cisco.com/en/US/products/ps5861/products_data_sheets_list.html

Melléklet

1. melléklet: A különböző EAP típusok összehasonlítása

EAP típus	Leírás
EAP-MD5 (Message-Digest5)	Az EAP-MD5 egy kihívásos hitelesítési protokoll (CHAP), mely a hitelesítéshez jelszót és felhasználói nevet igényel. Kis számítási teljesítménnyel jár a használata és nem igényel kulcs/tanúsítvány infrastruktúrát. Gyakorlatilag megegyezik a PPP CHAP protokollal. Kevéssé támogatott protokoll, mert sebezhető a nyerserő és a szótár-támadásokkal.
EAP-OTP (One Time Pad)	Hasonló az MD5 hitelesítéshez, de a kihívásra válaszként egyszeri jelszót alkalmaz (OTP, One Time Password). Ezt a megoldást széleskörűen használják a VPN és PPP technológiákat használó hálózatokban, azonban a vezeték nélküli hálózatokban nem annyira elterjedt.
EAP-GTC	Hasonló az EAP-OTP-hez, de OTP helyett (hardver) token-kártyát használ.
Lightweight EAP (LEAP)	Cisco által kifejlesztett hitelesítési eljárás, melynél felhasználói név/jelszó páros szükséges a hitelesítő szervernek (RADIUS). Nem tekinthető biztonságos hitelesítő eljárásnak.
EAP-TLS (Transport Layer Security)	Az EAP-TLS egy kölcsönös hitelesítést biztosít, úgy hogy egy titkosított szállítási csatornát biztosít, így téve lehetővé a kulcsok dinamikus cseréjét. A hitelesítési folyamat során a kérvényező és a hitelesítő szerver a publikus kulcsú infrastruktúrára támaszkodik (PKI) és mindkettőnek rendelkeznie kell tanúsítvánnyal. Az EAP-TLS a TLS protokollon alapul.
EAP-TTLS (Tunneled TLS)	Hasonló az EAP-TLS-hez, de a kliens hitelesítése a biztonságos szállító csatorna kiépítése után történik meg. Titkosított TLS-csatornát hoz létre a hitelesítési adatok biztonságos továbbítására és a TLS-csatornán belül bármilyen más hitelesítési módszer használható.
PEAP (Protected EAP)	A PEAP a TLS protokollal együtt hoz létre egy titkosított csatornát. Csak szerveroldali tanúsítványt igényel. A következőket nyújtja: egy TLS-csatornát, amely védelmet biztosít az ügyfél és a kiszolgáló közötti EAP módszeregyeztetéshez; támogatást az üzenetek darabolásához és összeillesztéséhez, lehetővé téve az olyan EAP-típusok használatára, amelyek nem rendelkeznek ezzel a szolgáltatással; védelmet a nem hitelesített vezeték nélküli hozzáférési pontok felállítása ellen abban a pillanatban, ahogy az EAP-ügyfél hitelesíti a hálózati házirend-kiszolgáló által nyújtott tanúsítványt. A Microsoft és a Cisco közös fejlesztése.
EAP-FAST	Az különböző EAP protokollok között a legbiztonságosabb és legátfogóbb protokoll. Biztonságosnak bizonyult a szótár-támadással szemben. A EAP-FAST egy megerősített

(Flexible Authentication via Secure Tunneling)	LEAP, melyben jobb titkosítási mechanizmust implementáltak. Az EAP-FAST minimalizálja a hardverigényt amellett, hogy csökkenti a man-in-the-middle (közbülső ember) támadás kockázatát. A hitelesítési folyamat biztonságáért az EAP-FAST egy titkos, osztott kulcsot használ a kliens és a hitelesítő szerver között, melynek neve Protected Access Credential Key (PAC-Key, Védett Hozzáférési Kulcs). Ez egy összetett kulcs, mely egy 32 bájtos, szerver által tárolt kulcsból és PAC információkból (metaadatok) áll.

Forrás: Orosz–Sztrik–Soong [2005] és Sankar et al. [2004] alapján saját összeállítás.