Debreceni Egyetem
Informatika kar

VEZETÉK NÉLKÜLI HÁLÓZATOK BIZTONSÁGI KÉRDÉSEI

Témavezető:
dr. Krausz Tamás
Számítástechnikai munkatárs

Készítette:
Jobbágy Boldizsár
Programozó matematikus

Debrecen, 2007.

2. Bevezetés

A dolgozatom témaválasztásakor, arra törekedtem, hogy minél aktuálisabb témát dolgozzak fel az informatika témakörében, és természetesen arra is, hogy a jövőmre nézve minél hasznosabb információkra tegyek szert az adott probléma beható megismerése által. Nem titkolt célom, hogy diplomaszerzésem után, PDA-k programozásával szeretnék foglalkozni, és ezen belül is, a hálózati kapcsolatokat is kihasználó szoftverek fejlesztésében látom a legnagyobb kihívást.

Szakdolgozatom céljául egy olyan terület körbejárását tűztem ki, amely viszonylagos újszerűsége miatt, még igen képlékeny és ezzel együtt sok kérdőjelet tartalmaz. Mindig is érdekeltek azon tudomány területek, amelyek még nem tartalmaznak kiforrott, hosszú évek, évtizedek óta bevált, megfedhetetlen technikákat, technológiákat. A vezeték nélküli számítógépes hálózatoknak nem is a léte újdonság, hanem ezen rendszerek biztonsága az amely kérdéses. A köztudatban máig úgy él, hogy nem létezik megfelelő módszer az adataink ilyen módon történő biztonságos közlésére.

Ahogy elmélyültem a különböző módszerek megismerésében, egyre inkább beigazolódni látszott, hogy nem a rendszerek azok, amelyek nem állnak még készen a biztonságos működésre, hanem a felhasználók azok, akik az ismeret hiányában, nem élnek, vagy egész egyszerűen nem jól használják azokat a lehetőségeket (eszközöket) amelyek védelmeznék adataikat.

Ezen dolgozat terjedelméből kifolyólag, nem hivatott minden létező módszer aprólékos, minden részletébe menő ismertetésére, azonban talán alkalmas arra, hogy az informatikai alapismeretekkel rendelkező olvasónak „felnyissa a szemét”. Általános példákkal szolgál arra, hogy a vezeték nélküli hálózatot használó felhasználó – napról-napra egyre több ilyen van - egy kicsit jobban megismerje ezt a „vezeték nélküli világot”, annak minden előnyével és nem kevesebb buktatójával együtt. A 2. fejezetben bevezetésként, alap információkat gyűjtöttem össze a Wireless hálózatokról, jellemzem ezek méretük szerint csoportokba szedve. A (*vezeték nélküli lokális hálózat, WLAN*) az, amelyre egy kicsit részletesebben kitérek, itt megemlítve a jelenleg hivatalos szabványokat is. A 3.fejezet a dolgozat tárgyalási része, amely először is a biztonságos hálózat néhány alapfogalmát írja le, majd veszélyforrásként felsorolja a jellemző támadási formákat, majd ezen támadásokat kiküszöbölendő biztonsági mechanizmusok tárgyalása következik. Legnagyobb részletességgel a WEP-ről írtam, mivel a mai napig ezen technika támogatottsága a

legjellemzőbb. Ugyan nem sokkal ezután belátjuk gyengeségeit is, de alapvető biztonsági módszer, amelyet ismerni érdemes annak, akit egy kicsit is foglalkoztat a vezeték nélküli biztonság. Lesz szó az AES-ről, a Wi-Fi védett hozzáférésről, a virtuális magánhálózatokról, a MAC –szűrőkről és a Radius szerverekről is. Ezek után a biztonsági rendszabályok típusait járjuk körbe, és belátjuk ezek használatának fontosságát, mind vállalati szinten, mind pedig otthoni felhasználóként egyaránt. Végül pedig egy kis történelmi áttekintés következik érdekesség képen, hogy milyen állomási voltak a vezeték nélküli szabványnak addig, még elérte mai formáját.

2.1. A Wireless hálózatról általánosságban

Az utóbbi néhány évben mindennapi életünk részévé váltak a vezeték nélküli kommunikációs eszközök. A legelterjedtebb a mindenki által használt mobiltelefon, de egyre nagyobb számban vásárolunk mobil számítógépeket (laptopokat, Pocket PC-ket, PDA-kat), melyek hálózatba kötése túlságosan körülményes és bonyolult volna fixen telepített vezetékekkel ill. pont a fő erényüket, a mobilitásukat veszítenék el ez által. A mobilitás ma egy teljesen hétköznapi elvárás az informatikában, természetesen az eddig megszokott működés megtartása mellett. A mai értelemben vett mobil ad hoc hálózatok kialakulása a 2. világháború idejére tehető vissza. A harcmezőkön nem volt előre megépített infrastruktúra, pedig kommunikációra ott is nagyon nagy szükség volt. Ellenséges területen az egyik legnagyobb érték az idő, márpedig a kommunikációs hálózat kiépítésével járó idő igen komoly veszteség lehet. Egy más jellegű példa a mai ad hoc hálózatokra egy olyan konferencia hálózat, ahol csak néhány előadás kedvéért kéne kialakítani a kommunikációs rendszert, nem feltétlenül kifizetődő a kábelezéssel járó munka és anyagi ráfordítás.

A mobil számítógépeknek az asztali gépekhez viszonyítva viszonylag kicsi az erőforrás kapacitásuk, ezért nagyon is ésszerű ezeket hálózatba kapcsolni, biztosítva ezzel az erőforrások (háttértár, nyomtató) közös elérését, használatát. Mint neve is mutatja, a **Wireless LAN**, vagyis a vezeték nélküli lokális hálózat egy olyan hálózati megoldás, amely a hagyományos LAN-tól (Local Area Network) elsősorban abban különbözik, hogy nem kell hozzá vezeték a jelek továbbítása céljából. Ehelyett a legtöbb esetben rádiófrekvencián, a levegőn át, kerülnek továbbításra az adatok. Ez a különbség rengeteg előnnyel jár hátrányuk viszont, hogy – a fizikai kapcsolatok hiánya és a rádiós csatorna jellege miatt – több potenciális támadásnak vannak kitéve, mint vezetékes társaik általában. Fontos tehát, hogy a vezeték nélküli hálózatok megfelelő védelmi mechanizmusokkal legyenek ellátva, melyek

minden körülmények között (azaz rosszindulatú támadások esetén is) biztosítják a biztonságos működést. Előnyként mindenek előtt megemlítendő, hogy megszűnik a helyhez kötöttség problémája a végberendezések (notebook, palmtop stb.) használói számára, másrészt elfelejthetjük ezáltal a kábelezés okozta gondokat, ezeken felül pedig egy ilyen vezeték nélkül kialakított hálózat olyan helyekre is „eljuthat", ahova a kábelek nem tudnának.

Ellentétben a hagyományos hálózatokkal, a vezeték nélküli alkalmi (un. ad hoc) hálózatok rendelkeznek azzal az előnnyel, hogy nincs szükség infrastruktúra kiépítésére. Az egyenrangú résztvevők együttműködve valósítják meg a kommunikációt. A hálózat felépítése is egyszerűbbé és gyorsabbá válik, és hosszútávon jóval alacsonyabb a működtetés költsége, ezért a relatívan drágább induló befektetések (speciális hardverek költségei) is hamar megtérülhetnek, valamint sokféle hálózati topológia is könnyen kialakítható az igényeknek megfelelően.

Napjainkban már hazánkban sem számít luxusnak a vezeték nélküli hálózat, az USA-ban még elterjedtebb, aminek velejárója az is, hogy ott a szükséges berendezések ára is csak tört része az európai áraknak. Manapság érdemes hosszú távú alternatívaként figyelembe venni ezt a lehetőséget, főleg cégek esetében, de egy magánember életében is megjelenhet a Wireless hálózat. Már hazánkban is a legtöbb cég rendelkezik vele, és az egyetemi kollégiumok, campusok területén is nagyon elterjedt a használata. Adott esetben az előadótermek is le vannak fedve, a diákok és tanárok magukkal hordják a laptopjukat, és mindenhonnan elérik a fontos információkat. Kórházakban is előnyös, ha az orvosok és nővérek olyan kézi számítógépekkel vannak felszerelkezve, amelyek egy ilyen hálózat segítségével folyamatosan, bárhol friss információkat szolgáltatnak a betegekről. Természetesen cégek esetében is nagyon előnyös, ha egy (meeting), tárgyalás során a kézi számítógépről bármelyik más teremben is elérhetőek, bemutathatóak a hálózaton vagy az Interneten található legfrissebb adatok (és persze, nem kell kábelkötegeken átbukdácsolni).

Természetesen a mobiltelefon is a vezeték nélküli kommunikáció egyik típusa és napjainkban rendkívül népszerű a világszerte egymással beszélgető emberek körében. A vezeték nélküli kommunikációs rendszerek számos típusa létezik, de a vezeték nélküli hálózat egyik megkülönböztető jellemzője, hogy itt a kommunikáció számítástechnikai eszközök között zajlik. Ilyen eszköz többek között a kézi számítógép vagy az ún. digitális-személyi titkár, (personal digital assistant, PDA), a laptop, a személyi számítógép, a szerver a nyomtató. A számítástechnikai eszközök processzorral, memóriával és meghatározott típusú hálózathoz való csatlakozásra alkalmas egységgel rendelkeznek. A jövőben a legtöbb elektronikai eszköz lehetőséget teremt majd a vezeték nélküli hálózati összeköttetés létesítésére.

Akárcsak a rézvezetékes vagy az optikai fényvezető szálas hálózat, a vezeték nélküli hálózat is számítástechnikai eszközök között továbbít információt. Az információ e-mail üzenetek, weblapok, adatbázis-rekordok, letöltés alatt álló videó- vagy hangadatok formájában jelentkezhet.

2. 2. Vezeték nélküli hálózatok méretük szerinti csoportosítása

A vezeték nélküli hálózatok az általuk lefedett fizikai terület méretétől függően különböző csoportokba sorolhatók. Alábbi típusai eltérő felhasználói követelményeknek tesznek eleget:

2. 2.1.Vezeték nélküli személyi hálózat (PAN)

A vezeték nélküli személyi hálózatok viszonylag kis hatótávolsággal (körülbelül 15m) rendelkeznek és leghatékonyabban egy kisméretű szobában vagy az ember mozgásterében felmerülő igények kielégítésére alkalmasak. A vezeték nélküli személyi hálózatok teljesítménye mérsékelt, adatátviteli sebessége legfeljebb 2 Mb/s, azonban ez már elég figyelemre méltó teljesítmény ahhoz, hogy a vezetékes módszert leváltsa, akár kényelmi megfontolásból is. A legtöbb vezeték nélküli személyi hálózat rádióhullámot használ az információ levegőben történő továbbítására. A Bluetooth-szabvány például olyan vezeték nélküli személyi hálózat működését specifikálja, amely 2,4GHz-es frekvenciasávban, körülbelül 15m-es körzetben működik. Az IEEE (*Institute of Electrical and Electronics Engineers – Villamos és Elektronikai Mérnökök intézete*) 802.15 szabványa is tartalmazza a Bluetooth specifikációját a vezeték nélküli személyi hálózatokra vonatkozóan. Egyes hálózatok ebben a kategóriában, infravörös fényt használnak az információ egyik pontból másik pontba történő továbbításához. A közvetlenül továbbított infravörös nyalábok használatát az IrDA (*Infrared Data Association – Infravörös Adattársaság*) specifikációja írja le, melynek segítségével körülbelül 1m távolságra akár 4 Mb/s adatátviteli sebességgel lehet adatokat továbbítani. A szakdolgozat fő témája a biztonság. Ezen hálózat típus esetén nem indokolt veszélyforrásokról beszélnünk, ugyanis ilyen kis hatótávolságon belül, nem számíthatunk támadásokra. Ez a hálózat típus elsősorban olyan személyes funkciókat céloz meg, mint a kézi számítógép és a laptop kommunikációja, ill. mobiltelefon és laptop adatcseréje, de nem ritkán a személyi számítógép és annak valamilyen perifériája közötti kommunikáció.

2. 2.2.Vezeték nélküli lokális hálózat (LAN)

A vezeték nélküli lokális hálózatok irodaépületek, gyárak, egyetemek, kollégiumok és lakások belsejében és környezetében nagy adatátviteli sebességet biztosítanak. A cégek például azért létesítenek vezeték nélküli lokális hálózatot, hogy biztosítsák a laptopok mobil hozzáférését a vállalati alkalmazásokhoz. Ilyen rendszerrel a felhasználó a hálózati szolgáltatásokat az irodájától távol, például konferenciateremből vagy egyéb helyekről is igénybe veheti. Az alkalmazottak munkája ez által sokkal hatékonyabbá tehető, ha irodájuktól távol kell másokkal együtt dolgozniuk.

A vezeték nélküli lokális hálózatok számára nem okoz nehézséget olyan adatátviteli sebesség biztosítása, amely fejlett alkalmazások zökkenőmentes futtatását teszi lehetővé. Például egy ilyen hálózattípus felhasználói, könnyen megtekinthetnek egy elektronikus levélhez csatolt nagyméretű fájlt vagy egy szerverről letöltött videó-fájlt. A maximális 54 Mb/s adatátviteli sebességnek köszönhetően a vezeték nélküli lokális hálózat szinte bármilyen irodai vagy otthoni hálózati alkalmazáshoz megfelelő. A vezeték nélküli LAN -ok teljesítménye, összetevői, költségei valamint üzemeltetésének tekintetében hasonlóak a hagyományos, vezetékes *Ethernet-hálózatokhoz*. A vezeték nélküli lokális hálózati adapterek laptopokban történő széles körű felhasználása miatt a legtöbb nyilvános, vezeték nélküli hálózati szolgáltató vezeték nélküli LAN -okat is igénybe vesz a mobil, szélessávú Internet-hozzáférés biztosítására. A felhasználók az úgynevezett forrópontokon (*hotspot*) vagy a nyilvános, vezeték nélküli lokális hálózat hatókörén belül (pl. repülőtéren vagy szállodában) meghatározott díj ellenében hozzáférhetnek elektronikus leveleikhez és böngészhetnek az Interneten. A nyilvános vezeték nélküli LAN -ok gyors fejlődése miatt az Internet elérhetővé válik azokon a helyeken, ahol az emberek tömegesen jelennek meg.

Tekintsük át a WLAN-ok jellemző szabványait: A vezeték nélküli hálózatok az évek során több szabvánnyal is gazdagodtak. A mai *hivatalos szabványok* (az adatátviteli képességet, sávszélességet tekintve) az *IEEE 802.11b, 802.11a,* és *802.11g*. Az IEEE (Institute of Electrical and Electronics Engineers) a nemzetközi szabványügyi szövetség, a 802.11 a Wi-Fi szabványrendszert a B, A és G betűk pedig a konkrét szabványt jelzik. Lássuk ezeket a szabványokat kicsit bővebben.

802.11b

Ez a szabvány a 2,4 GHz -es nyílt frekvenciatartományt használja, ahogy mikrohullámú sütőnk, vezeték nélkül telefonunk és egyéb hétköznapi vezeték nélküli eszközeink is. Ennek megfelelően a különböző eszközök rádióhullámai interferenciát okozhatnak (interferálhatnak), magyarul zavarhatják egymást. Sávszélességét tekintve *11Mbit/másodperc* (megabit: Mbit) *elméleti maximum adatátviteli sebességre* képes, ami *a gyakorlatban 4-6Mbit*-et jelent. Ez jóval gyorsabb, mint például DSL kapcsolatunk sebessége, azaz bőven elegendő több kliens egyidejű Internet kiszolgálására, komolyabb adatforgalom esetén (zenehallgatás, filmnézés, fájl-másolás stb.) azonban már kevés lehet. Előnye viszont, hogy manapság már nagyon elterjedt és nagyon olcsó, ezért találkozunk vele a legtöbb elektronikai eszközben (telefonokban, PDA -kban stb.). Hatótávolsága 30-50 méter épületben, 1 km épületen kívül az Access Point -ra történő tiszta rálátás esetén.

802.11a

A 802.11a szabvány szinte egyszerre jelent meg a 802.11b -vel, amelytől azonban több aspektusban is eltér. Legfontosabb, hogy az *5GHz -es tartományban üzemel*, tehát szokásos eszközeink, amelyek rádiófrekvenciás hullámokat bocsátanak ki, nem zavarják az adatforgalmunkat. A megemelt frekvenciából adódóan sávszélessége is növekedett, *maximum 54Mbit/másodperc* (a gyakorlatban 21-22Mbit), viszont a nagyobb frekvenciájú rádióhullámok tulajdonságainak köszönhetően (könnyebben elakadnak a különböző tárgyakban, falakon) *hatótávolsága kisebb*, mindössze 10-25 méter épületen belül. Ezt ellensúlyozza, hogy az 5GHz-es tartományban több, egymást nem átfedő "csatornát" vehetünk akár egyszerre is igénybe, azaz növelhetjük konkrét sávszélességünket, lehetővé téve, hogy egyszerre több felhasználó nyugodtan nézhessen filmet (streaming) vagy másolhasson nagy fájlokat anélkül, hogy jelentős sebességcsökkenést érzékelne.

802.11g

A "legfrissebb" hivatalos IEEE vezeték nélküli szabvány, ugyanabban a tartományban üzemel, mint a 802.11b, azonban *megnövelt, 54Mbit/másodperc sávszélességgel rendelkezik*, ami gyakorlatilag 15-20Mbit -et jelent a valóságban, tehát az *A* változattal azonos képességű.

Hatótávolsága viszont a *B* változatéval megegyező, épületen belül 30-50 méter. Ez a szabvány visszafelé kompatibilis a *B* változattal, azaz egy *G* -s eszköz képes kommunikálni egy *B* -s Access Point -tal illetve egy *B* -s eszköz is egy *G* -s Access Point -tal.

2.2.3.Vezeték nélküli nagyvárosi hálózat (MAN)

A vezeték nélküli nagyvárosi hálózatok város nagyságú területeket fednek le. Ilyen hálózattípust használhatnak, pl. a kórházak a központi épületük és egy távoli klinika között szükséges adatátvitel biztosítására. Egy villamosenergia-szolgáltató cég pedig azért létesít vezeték nélküli MAN hálózatot egy adott városrészben, hogy lehetővé tegye a megrendelések különböző helyekről történő feladását. Így ez a hálózat típus kifejezetten alkalmas a meglévő hálózati infrastruktúra összekapcsolására, és lehetővé teszi a mobilfelhasználók számára, hogy a meglévő hálózati infrastruktúrájuk felhasználásával kommunikáljanak egymással.
A vezeték nélküli Internet-szolgáltatók (wireless internet service provider, WISP) vezeték nélküli nagyvárosi hálózatokat létesítenek a városokban és vidéken annak érdekében, hogy állandó vezeték nélküli összeköttetést biztosítsanak az otthonok és a vállalatok részére. A vezeték nélkül nagyvárosi hálózat rendkívül előnyös ott, ahol a hagyományos vezetékes összeköttetés, például a digitális előfizetői vonalak (digital subscriber line, DSL) kiépítése vagy vezetékes modemek alkalmazása nem megoldható, pl. szolgalmi jogból eredő korlátozások miatt, túl költséges lenne.
Adatátviteli sebességük változó. Az épületek között az adatokat infravörös fény segítségével továbbító összeköttetés meghaladja a 100 Gb/s-ot, ugyanakkor egy körülbelül 30 km-es rádióhullámú összeköttetés esetén az adatátviteli sebesség legfeljebb 100 Kb/s lehet. Egyes forgalmazók az IEEE 802.11 szabványt tekintik a vezeték nélküli MAN -ok alapjának, de az újabbak többnyire a viszonylag új IEEE 802.16 szerinti rendszereket forgalmaz, melynek adatátviteli sebessége ésszerű távolságokon Mb/s –os sebességet produkál. Ennek köszönhetően az IEEE 802.16 szabvány valószínűleg általánosan elfogadott szabvánnyá válik majd a vezeték nélküli nagyvárosi hálózatok körében.

2.2.4.Vezeték nélküli nagy kiterjedésű hálózat (WAN)

A vezeték nélküli nagy kiterjedésű hálózatok nagy területet, például egy országot, vagy kontinenst, lefedő mobilalkalmazásokat tesznek lehetővé. A vezeték nélküli WAN –ok

teljesítménye kicsi, adatátviteli sebességük legfeljebb 170 Kb/s, de tipikusan csak 56 Kb/s. Ez a teljesítményszint hasonló a tárcsázásos telefonmodemekéhez.
Ezen hálózattípusnál számos, egymással versenyben álló szabványt alkalmaznak, melyek csak lassan fejlődnek. A celluláris datagram szolgálat (*cellular digital packet data, DCPD*) pl. egy olyan régebbi technológia, amely analóg mobiltelefon-rendszerekben az adatok 19,2 Kb/s adatátviteli sebességgel történő továbbítását teszi lehetővé. Néhány cég még ma is kínál CDPD -szolgáltatást az Egyesült-Államokban, azonban ez a technológia egyre inkább elavul, mivel a távközlési szolgáltatók a harmadik generációs (3G) távközlési rendszerek irányába fordulnak, ahol az elérhető adatátviteli sebességek a Mb/s–os nagyságrendbe esnek.

Az előbb felsorolt vezeték nélküli hálózat típusok jól kiegészítik egymást, miközben eltérő igényeket elégítenek ki. Időnként mégis nehéz különbséget tenni az egyes típusok között. Az épületen belül működő vezeték nélküli lokális hálózat, pl. összeköttetést biztosíthat kézi számítógép és asztali számítógép között is, akárcsak a vezeték nélküli személyi hálózat. A technológiák és a szabványok ugyanakkor egyértelműen elhatárolják egymástól a különböző hálózat típusokat.

3. Tárgyalási rész

3. 1. A biztonságos hálózat alapfogalmai

Napjainkra már számos olyan szempont létezik, amely a biztonságos kommunikációs rendszerekkel szemben elvárhatóak. Ezek az igények a hagyományos hálózatok lehetőségeihez lettek formálva. Az ad hoc rendszerek működése gyökeresen más szemléletet rejt, azonban a biztonságos kommunikáció igénye ugyanazon követelményeket támasztja. A következőkben tehát azokat a követelményeket ismertetem, melyeket egy biztonságos rendszernek nyújtania kell.

Információ titkosságának (*confidentiality*) nevezzük azt a funkciót, melyben az információ csak azokhoz a résztvevőkhöz jut el, akiknek a küldő szánta. Mivel az információk a hálózatban résztvevők továbbításával jutnak célba, a bizalmas adatok védelme nélkülözhetetlen. A védendő információk nem csak a felhasználók által küldött adatok lehetnek, hanem például a rendszer jelzései is, melyek felhasználásával a támadó hasznos információkhoz juthat (pl. eszköz lokalizálása).

Integritás (*integrity*) az a követelmény, mely biztosítja, hogy az adatok átvitele során történt változásokra fény derüljön. Változást okozhatnak természetes környezeti hatások, mint például az átviteli csatorna gyenge minősége, de egy támadó célja is lehet üzenetek megváltoztatása, új üzenetek beszúrása vagy üzenetek törlése.

A ***hitelesítés*** (*authentication*) során az üzenet vagy a küldő személye lesz azonosítva. Biztonságos kommunikáció felépítésekor fontos bizonyosságot nyerni a másik fél személyéről, hogy kizárjuk a megszemélyesítés lehetőségét.

Letagadhatatlanságnak (*non-repudiation*) nevezzük azt a követelményt, mely garantálja, hogy a kommunikáció során az üzenetek akár később is meghatározzák a küldő személyét. Ennek segítségével az adott résztvevő és tevékenysége azonosíthatóvá válik, mely utólagos nyomozási vagy bizonyítási eljárásokhoz szükséges lehet.

Elérhetőségnek (*availability*) nevezzük a hálózat elemeinek és a hálózat szolgáltatásainak folyamatos rendelkezésre állását. A rendszer működését veszélyeztetik a meghibásodások, a környezeti hatások és szándékos támadások is. Szükség lehet ezeken kívül egyéb biztonsági szolgáltatásokra is, mint például a hozzáférés védelem (*authorization*), ami a rendszer erőforrásaihoz való hozzáférést korlátozza.

3.2.A mobil Ad hoc hálózatok veszélyforrásai általában

A mobil ad hoc hálózatok biztonsági szempontból a hagyományos hálózatokhoz képest újabb veszélyeket rejtenek. Ezeket a tényezőket nézzük meg a következőkben.
A tapasztalt *hacker*, de még egy alkalmi lehallgató személy (*snooper*) is könnyedén monitorozhatja a védelemmel el nem látott, vezeték nélkül továbbított adatcsomagokat valamilyen eszköz, pl. *AirMagnet* vagy *AiroPeek* segítségével, amely teljes mértékben képes feltárni a vezeték nélkül továbbított adatcsomagok tartalmát. A tolvajok a hálózat vezeték nélküli részében zajló minden tranzakciót monitorozni tudnak a lokális hálózatot használó épülettől akár több száz méterre is. A mobil ad hoc hálózatok egységei rendszerint hordozható, kisméretű, kézi készülékek, melyek korlátozott CPU-, memória-, és telepkapacitással rendelkeznek. A telep élettartamának megnövelése céljából minimalizálni kell az erőforrás-igényes algoritmusok futtatását, így kompromisszumokat követel például a

kommunikáció során alkalmazott kriptográfiai műveletek megválasztása is. Túl egyszerű algoritmus esetén azonban megnőhet akár a kódtöréses támadások esélye.

A telepkímélés egy másik fontos mechanizmusa a rádióadó, illetve akár az egész készülék ki-, vagy készenléti állapotba kapcsolása akkor, amikor nincs rá szükség. Egy lehetséges támadási forma az olyan szolgáltatásbénító (*Denial of Service - DoS*) támadás, melynek célja pont a résztvevők energiaforrásainak pazarlása (*sleep deprivation*). Ekkor a támadó a készüléket folyamatosan aktivált állapotban tartja. Fennáll a CPU elleni DoS támadás veszélye is, például, amikor egy támadó nagy számításigényű műveletek elvégzésére kötelezi a másik résztvevőt. Ekkor a számolással elfoglalt egység nem tud válaszolni, elérhetetlen lesz. Nehézségeket okozhat a memória korlátossága is, mivel gátat szab például a tárolható kulcsok mennyiségének, illetve a nem megbízható egységek listájának hosszára is. Mivel ad hoc rendszerekben a csomagtovábbítás a résztvevők együttműködésén alapszik, ezért felmerülő kérések esetén válaszolni kell. Így támadásnak minősül az ebben való részvétel önző megtagadása is, azaz ha a támadó a hozzá érkező csomagokat nem továbbítja. Hordozható készülék könnyen illetéktelen személy kezébe juthat (pl. lopás), így számítani lehet arra is, hogy egy megbízott résztvevő készüléke egyszerre csak támadóként kezd viselkedni. A készülékek kis méret és súlyigényének következtében csak gyenge fizikai védelemmel látható el, így egy megszerzett készüléken hardver, illetve szoftvermódosítások végezhetőek. A felhasználó tárolt bizalmas információi rossz kezekbe kerülhetnek (pl. titkos kulcs), de a szoftver módosításaival a támadó vírust vagy trójai falovat is telepíthet az eszközbe.

Az intranetek tűzfallal történő védelme sem megvalósítható, mivel a belső és külső hálózatok érintkezési pontjai nem egyértelműek. Mert ha egy épületben valaki rádiós kommunikációt használ, akkor az ő kommunikációja az épületen, a tűzfalon kívül is hallható lehet. Az osztott médium megzavarása DoS támadásként jöhet szóba. A csatorna elzajosításával az átviteli minőség lerontható, de akár teljesen használhatatlanná is tehető. A támadó által sugárzott zavaró jel csak nehezen választható el a csatorna természetes zajától. A csatornához való hozzáférés is együttműködést igényel, vagy szabályainak megsértése egy másik módja a kommunikáció megzavarásának. Az információk integritásának védelmére ezért szükség van. Egy támadó próbálkozhat az információk megváltoztatásával, vagy például új üzenetek beszúrásával az adatfolyamba, utazó csomagok teljes eltávolításával, de akár azok megváltoztatásával is.

A biztonságos kommunikáció igénye szükségessé teszi olyan üzenetváltások meglétét, melyek futtatói a kommunikáció befejeztével meghatározott jellemzőkkel kell, hogy rendelkeznek. Biztonsági protokollok célja a résztvevők közötti titkos, illetve megfelelően

hitelesített kapcsolat felépítése, ezek feladatai körébe tartoznak még például a kapcsolathoz szükséges kulcsok előállításai, illetve kódoltan a megfelelően hitelesített résztvevőkhöz juttatása. Egy támadó az üzenetváltások megfigyelésével és a szerzett információk felhasználásával a protokoll működésébe úgy igyekszik beavatkozni, hogy azzal a futtató résztvevőket megtévessze, és így a futtatás befejeztével aláássa a feltételezett biztonságot. Egy ilyen támadó minden előre ismert, megszerezhető, illetve kikövetkeztethető információt felhasználhat, egyetlen korlátja a kriptográfiai algoritmusok által kódolt üzenetek olvasása. Ezzel tehát feltételezzük, hogy titkosítási algoritmusaink jól működők, feltörhetetlenek a támadó számára.

3.2.1.Jogosulatlan hozzáférés

Ha nem tesznek megfelelő óvintézkedéseket, a vállalat vezeték nélküli hálózatához az épületen kívül is bárki erőfeszítés nélkül hozzáférhet, mint a vezeték nélküli alkalmazások monitorozása esetén. Egy parkoló autóban ülve, pl. bárki kapcsolatba léphet az épületen belül elhelyezkedő vezeték nélküli bázisállomással. Sajnos sok vállalat alapértelmezésként beállított, biztonság nélküli bázisállomásokkal működteti vezeték nélküli hálózatát, így az alkalmazási szerverekhez nem nehéz hozzáférni. Ha támadást próbálnánk indítani a vezeték nélküli lokális hálózati hozzáférési pontok ellen, akkor egy átlagos városban azt tapasztalhatnánk, hogy 30 százalékuk semmilyen biztonsági intézkedést nem tesz, a merevlemezekhez és a felhasználói erőforrásokhoz bárki hozzáférhet, pl. Internet-összeköttetésen keresztül. A Microsoft® Windows XP operációs rendszer megkönnyíti a vezeték nélküli hálózathoz való csatlakozást, különösen nyilvános vezeték nélküli LAN-okból. Amikor a vezeték nélküli lokális hálózathoz laptopot csatlakoztatnak, a felhasználó bármelyik, ugyanahhoz a hálózathoz kapcsolódó laptophoz eljuthat. Személyi tűzfal (*firewall*) hiányában bárki kutakodhat merevlemezünkön. Ez a biztonság szempontjából óriási kockázatot jelent.

3. 2.2.Csaló hozzáférési pontok – rouge access point

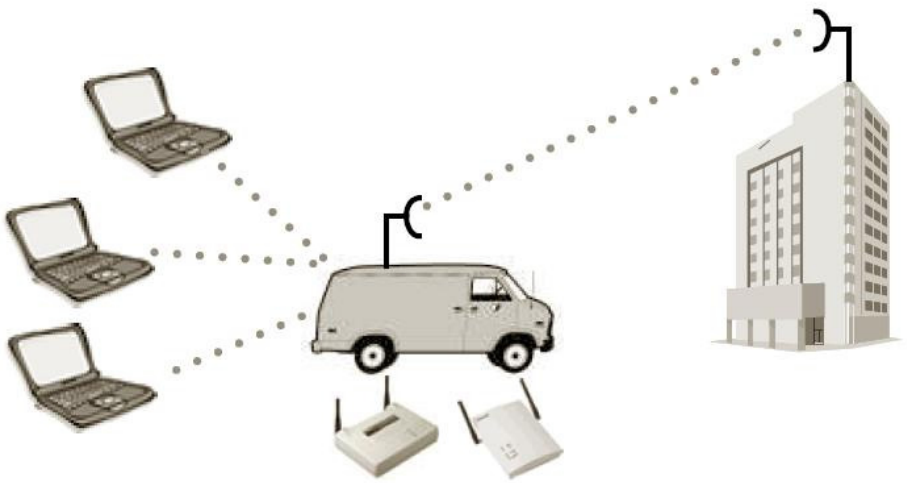
Ha minden biztonsági eszközt igénybe veszünk a hozzáférési pontokon, akkor is komoly veszélyt jelenthet csaló hozzáférési pontok csatlakoztatása a hálózathoz. A csaló hozzáférési pont engedély nélkül működtetett hálózati hozzáférési pontot jelent. Ilyen pontot hoz létre, pl. az alkalmazott, amikor irodájában a biztonsági előírások figyelembe vétele nélkül helyez üzembe egy hozzáférési pontot. A hackerek is létrehozhatnak csaló hozzáférési pontot az

épületen belül, kifejezetten azzal a céllal, hogy a vállalati hálózathoz a védelem nélküli hozzáférési ponton keresztül tudjanak csatlakozni. Ezért a vállalatoknak az ilyen csaló pontok esetleges megjelenését folyamatosan figyelniük kell. Ez a probléma független attól, hogy vezeték nélküli hálózatot használunk-e. Csaló hozzáférési pont a vezetékes Ethernet - hálózathoz is csatlakoztatható.

Az engedély nélküli hozzáférés megelőzése céljából a vezeték nélküli hálózatoknak kölcsönös hitelesítést kell végrehajtaniuk a klienseszközök és a hozzáférési pontok között. A hitelesítés nem más, mint egy személy vagy eszköz azonosságának igazolása. A vezeték nélküli hálózatokban olyan eljárásokat kell implementálni, amelyek a bázisállomások számára igazolják a klienseszközök azonosságát és viszont. Ezen kívül a hozzáférési pontokat is kapcsolókkal kell hitelesíteni azzal a céllal, hogy a csaló hozzáférési pont sikeres csatlakozását megakadályozzuk ez által.

3.2.3.Emberközpontú támadás – Man in the middle

A vezeték nélküli hálózatok kifejezetten gyenge pontja az emberközpontú támadás, amely során a *hacker* fiktív eszközként jelenik meg a felhasználó és a vezeték nélküli hálózat között.



1.ábra. Emberközpontú támadás

Az egyik leggyakoribb emberközpontú támadás az összes TCP/IP –hálózat által használt, szokásos címfeloldó protokoll (*address resolution protocol, ARP*) ellen irányul. Az ARP protokoll olyan alapvető funkció, amelyet a vezeték nélküli, vagy vezetékes hálózati interfészkártya a célállomás hálózati interfészkártyájához rendelt fizikai cím megszerzésére használ. A kártya fizikai címe köztudottan megegyezik a közeghozzáférés-vezérlő MAC címével, amit a gyártó a kártyában helyez el, és teljesen egyedi minden eszköz esetén. Az az

alkalmazási szoftver, amely adatokat kíván küldeni, ismeri ugyan a célállomás IP címét, de az adóoldali hálózati interfészkártyának az ARP-protokollt kell használnia a megfelelő fizikai cím megszerzéséhez.

Az ARP -protokoll hátránya, hogy könnyen becsapható, tehát a biztonság szempontjából komoly kockázatot jelent. A hacker pl. azzal csaphat be egy állomást, hogy a csaló hálózati eszközről olyan fiktív ARP -választ küld, amely törvényes hálózati eszköz IP -címét, de a csaló eszköz MAC –címét tartalmazza. Ekkor a hálózathoz kapcsolódó összes jogosan működő állomás automatikusan frissíti saját ARP –táblázatát a hamis leképezéssel. Ebből könnyen látható, hogy ezek az állomások a továbbiakban a csomagokat a törvényes hozzáférési pont vagy router helyett, a csaló eszköznek küldik majd el. A hacker ezáltal jelszavakhoz férhet hozzá, egyéb adatokat szerezhet meg, és ami talán a legrosszabb, másnak adhatja ki magát, akár egy igen magas beosztású felhasználónak is, ami által a vállalati szerverekbe is könnyedén beléphet.

Az ARP –protokoll becsapásával végzett emberközpontú támadás kivédése céljából a gyártók, mint például az OptimumPath, a biztonságos ARP- (*secure ARP, SARP*) protokollt implementálják, amely egy speciális biztonsági csatornát hoz létre az egyes kliensek és vezeték nélküli hozzáférési pontok vagy routerek között, amely minden olyan ARP –választ figyelmen kívül hagy, amely nem a csatorna másik végén lévő klienstől származik. Így csak jogos ARP –válaszok esetén történik meg az ARP –táblázatok módosítása. A SARP -protkollt alkalmazó állomást tehát nem lehet így megtéveszteni. Azonban ennek az új módszernek az alkalmazása az összes kliensen megköveteli ezen különleges szoftver telepítését, ezért nyilvános forrópontokon nem célszerű az alkalmazása, vállalatok esetében viszont nagyon is kifizetődő beruházást jelenthet.

3.2.4.Tükrözés - reflection

A trükk itt az, ami a névből is adódik, vagyis hogy a támadó egy résztvevőnél visszapattintja az üzenetet vagy annak egy részét. Ezzel az üzenet küldőjét lehet becsapni a helyes válasz feltárásával. Ez a támadás gyakran szimmetrikus helyzeteken alapul.

3.2.5.Jóslás - oracle

Ilyenkor a támadó a résztvevő által véletlenül felfedett információt használja. A támadó ráveszi a szereplőt, hogy a protokollból végrehajtson néhány üzenetváltást, ezáltal a támadó olyan adatokhoz jut hozzá, amihez másképp nem tudott volna. Ezekből az adatokból lehet jósolni az esetleges támadáshoz.

3.2.6.Visszajátszás - replay

A támadó folyamatosan figyeli a protokoll üzeneteit, és később ugyanazt az üzenetet visszajátssza. Ez akkor fordulhat elő, ha a protokoll nem tud különbséget tenni az üzenetek között, nem tartalmaz az adott üzenetre jellemző egyedi információt.

3.2.7.Összefésülés - interleave

Ez nagyon intelligens támadási forma, amikor a támadó két vagy több protokoll futás során kitalálja a protokoll átfedéseit. Sok esetben a támadó a jóslás és az összefésülés technikáját kombinálja, mely így sokkal eredményesebb.

3.2.8.Failures of forward secrecy

Valódi rendszerek működésében számítani kell a rendszer feltörésére. Ha egy támadó megszerez titkos kulcsokat, akkor ezek által, az összes e kulcsokkal titkosított üzenethez hozzájuthat. A rendszer teljes visszaállítása után is lehet a támadónál olyan információ, mely a rendszerre veszélyt jelenthet. Ezért az adatok titkosítására alkalmazott kulcsokat nem szabad újabb kulcsok bizalmas átvitelére használni, hanem erre külön kulcsot kell létrehozni.

3.2.9.Algebrai támadás

A kriptográfiai eljárások gyakran megfelelnek bizonyos algebrai szabályoknak. Erre példa a kizáró vagy művelettel való (*Vernam*) titkosítás, amikor is két azonos kulccsal titkosított üzenet kizáró vagy műveletének eredménye azonos lesz a két üzenet kizáró vagy kapcsolatával. Ezek közül így az egyik ismeretében következtetni lehet a másikra, valamint a használt kulcsra is.

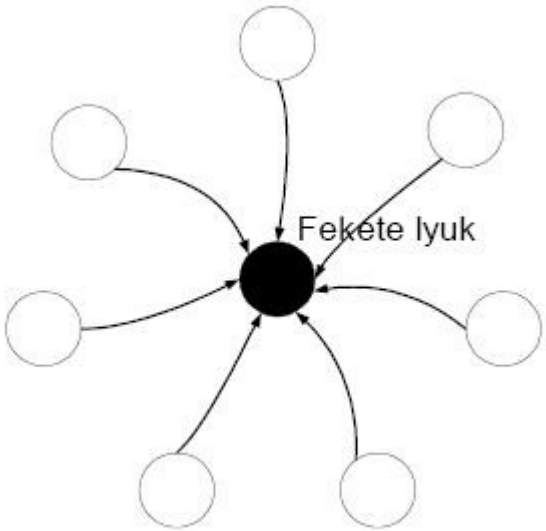
Az ad hoc hálózatok teljesen elosztott rendszerek, ahol nincsen központi elem. Így nincsen a rendszernek kiemelten érzékeny résztvevője, ám nem támaszkodhatunk központi segítségre sem. Nincsen teljesen megbízható pont a hálózatban, amely hiteles információkat szolgáltatna. A hagyományos rendszerekben elérhető és ezért széles körben alkalmazott hitelesítő központ hiányában a résztvevők megszemélyesítése komoly fenyegetést jelent.

Fokozott problémát jelent ez, az első találkozáskor történő azonosításra. Végpont megszemélyesítésről beszélünk, amikor egy támadó másnak adja ki magát, mint aki valójában. Nem csak végpontokat lehet megszemélyesíteni, hanem a közbülső résztvevőket is. *Man in the Middle* támadáskor a támadó az útvonalba épülve a címzettnek adja ki magát, így tévesztve meg a küldőt.

3.2.10.Útvonal-választó protokollokra irányuló támadások

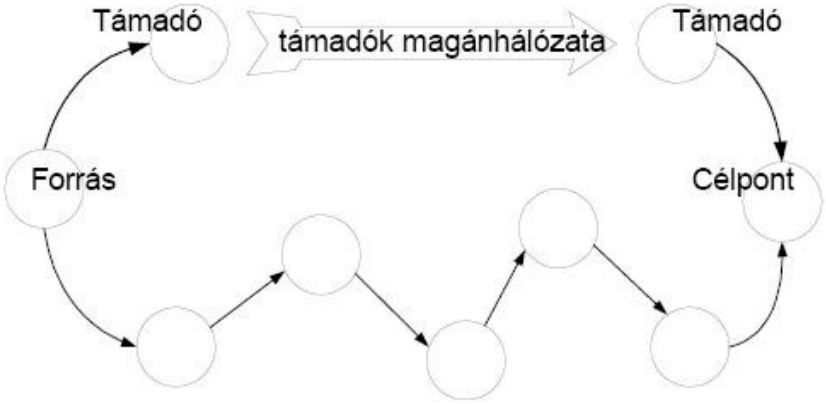
A mobil ad hoc hálózatok nem rendelkeznek fix infrastruktúrával, felépítésük idővel dinamikusan változik. Ennek következtében olyan útvonal-választási megoldásokra van szükség, melyek követni tudják a bekövetkező változásokat. A pillanatnyi architektúra feltérképezése, illetve a csomagok célba juttatása a résztvevők közös információjával és együttműködésével történhet. Így jelentős zavarokat okozhat az, ha egy támadó téves információkkal árasztja el és téveszti meg a hálózatot. A mobil ad hoc hálózatokra irányuló támadások jelentős része az útvonalválasztás mechanizmusát támadja, ezek az utazó csomagok eltérítését hivatottak elérni. A *man in the middle* esetében tárgyalt példán túl gyakori támadási módszer, amikor a támadó téves útvonal információk küldésével egy hurkot hoz létre az útvonalban. Az ebbe bekerülő csomagok sohasem érnek célba, körbe-körbe utaznak, miközben a rendszer energiáját és sávszélességét pazarolják.

Másik egyszerű példa olyan *fekete lyuk* kialakítása, mely minden csomagot elnyel. A támadó elérheti ezt is meghamisított útvonal információkkal, mindössze minden csomagot saját magára kell irányítania, majd az érkező csomagokat figyelmen kívül hagyni.



2.ábra: A fekete lyuk

A fekete lyuk speciális esete a *szürke lyuk*, mely szelektíven válogathat a csomagok között, a támadó tehát szűrést végezhet. Szintén útvonal manipulálással elérhetőek az optimálisnál jóval kedvezőtlenebb utak. Szélsőséges esetben a hálózat akár független tartományokra is darabolható, vagyis a résztvevők különböző halmazai nem érhetik el egymást.
Gratitous detour-nak nevezzük, amikor egy támadó a rajta keresztülvezető, egyébként rövid útvonalat virtuális résztvevők beiktatásával hosszabbnak, előnytelenebbnek tüntet fel. Több útvonal-választási mechanizmus is használ valamiféle feketelistát a rosszindulatú résztvevőkről. Egy támadó célja lehet a jó résztvevőknek rossz színben való feltüntetése hamis információk terjesztésével. Ezáltal ez is felhasználható támadási célra.
Egy trükkösebb támadás a *wormhole* támadás.



3.ábra: A Wormhole támadás

Ennek lényege, hogy két támadó egység egy előre felépített magánhálózaton sokkal gyorsabban átvihet információt, mint az éppen akkor utat kereső többi résztvevő. A támadás során tehát a felépítendő útvonal egy részét magánhálózatukkal áthidalják a támadók, így sokkal gyorsabbnak fog tűnni, a felépülő út tartalmazni fogja a támadókat.

3.2.11.Szolgáltatás megtagadás – denial of service, DoS

A szolgáltatásmegtagadásra (*denial of service, DoS*) irányuló támadás megbéníthatja, vagy működésképtelenné teheti a vezeték nélküli hálózatot. Ezen támadási forma egyik formája a nyers erő alkalmazása. Például a csomagokkal történő elárasztás, amikor a csomagok a hálózat összes erőforrását lekötik és a hálózatot leállásra kényszerítik. Az Internetről beszerezhetők olyan eszközök, amelyek a *hackerek* számára lehetővé teszik, hogy vezeték nélküli hálózatokat árasszanak el. A *hacker* úgy is végrehajthat szolgáltatásmegtagadásra irányuló, nyers erőt alkalmazó támadást, hogy a hálózat más számítógépeiről

hasznavehetetlen csomagokat küld a szervernek. Ez jelentősen növeli a hálózat terhelését, és elveszi a sávszélességet a jogos felhasználók elől.

A legtöbb vezeték nélküli hálózat – különösen a vivőérzékelésen alapuló hozzáférést alkalmazó hálózat – leállításának másik módja, hogy erős rádiójellel minden más rádióhullámot elnyomnak, és ez által a hozzáférési pontok és a rádiófrekvenciás kártyák használhatatlanná válnak. A hálózat erős rádiójelekkel történő megzavarása azonban kockázatos a támadó számára, ugyanis egy ilyen nagyteljesítményű adókészülék könnyen bemérhető, és ez által a helye meghatározható.

Vannak olyan biztonsági mechanizmusok, amelyek a szolgáltatás megtagadásra vonatokozó támadások elsődleges célpontjai. Ilyen például a hamarosan tárgyalásra kerülő Wi-Fi védett hozzáférésnek (*Wi-Fi protected access, WPA*) is, amely matematikai algoritmusokat használ a hálózathoz csatlakozó felhasználók hitelesítésére. Ha a felhasználó belép és egy másodpercen belül két olyan csomagot is küld, amely illetéktelen adatokat tartalmaz, a WPA támadást feltételez és leáll.

Láthattuk, hogy az ad hoc hálózatok nagyon sok veszélynek vannak kitéve. A biztonságos kommunikáció megvalósításához olyan megoldásokat kell alkalmazni, melyek egy támadó ellen sikeresen meg tudják védeni a hálózatot. A következő fejezetben áttekintünk ezen mechanizmusok közül néhányat.

3.3. Biztonsági mechanizmusok bemutatása

A WLAN -hálózatok védelméhez az eredeti 802.11 specifikáció három mechanizmust használ:

1. ***A Service Set Identifier (SSID)*** egy sima jelszó, ami azonosítja a vezeték nélküli hálózatot. A klienseknek muszáj beállítaniuk a korrekt SSID-t, hogy kapcsolódni tudjanak a WLAN hoz.
2. A ***MAC-address szűrés*** a számítógépek WLAN -elérését a WLAN minden egyes access point-jához készített listával (ACL).
3. A ***WEP*** egy titkosítási séma, ami védi a WLAN -adatfolyamokat az access point és a kliens között, mivel ezt előírja a 802.11 szabvány.

Ezek önmagukban nem elegendőek. A rendszergazda dolga eldönteni, hogy milyen biztonsági (titkosító) szabvány mellett dönt az alapelemeken fölül.

A titkosítás során az adatcsomagok bitjeit úgy módosítják, hogy a kommunikációt lehallgató személyek ne tudják az adatokat, például a hitelkártyaszámokat dekódolni. A titkosítás előtt álló adatokat nyílt szövegnek nevezik. A nyílt szöveget viszonylag könnyű dekódolni számítógépes hibák felderítésére szolgáló (*sniffing*) eszközök segítségével. A titkosítás a nyílt szöveget olyan titkos szöveggé alakítja át, amelyet csak a megfelelő titkos kulcs használatával lehet dekódolni.

IEEE 802.1x: egy biztonsági szabvány, amely portalapú hitelesítésen és dinamikus osztott-kulcsú WEP -kódoláson alapul. Dinamikus kulcsot használ a WEP -hitelesítés által alkalmazott statikus kulcs helyett, és megköveteli a hitelesítési protokollt a hitelesítési folyamat során. Hogy hitelesítve tudjon dolgozni, a felhasználónak az access point-on keresztül kell kapcsolódnia (tehát a peer-to-peer vagy ad hoc mód teljesen ki van zárva), amely kapcsolódva ráadásul egy RADIUS -szerver segítségével végzi az authentikációt.

3.1.1. A WEP

Az IEEE 802.11 vezeték nélküli LAN szabvány tervezői kezdettől fogva fontosnak tartották a biztonságot. Ezért már a 802.11 korai verziója is tartalmazott biztonsági mechanizmusokat, melyek összességét WEP-nek (*Wired Equivalent Privacy*) nevezték el. Ahogy arra a név is utal, a WEP célja az, hogy a vezeték nélküli hálózatot *legalább* olyan biztonságossá tegye, mint egy – különösebb biztonsági kiegészítésekkel nem rendelkező – vezetékes hálózat. Ha például egy támadó egy vezetékes Ethernet hálózathoz szeretne csatlakozni, akkor hozzá kell férnie az Ethernet hub-hoz. Mivel azonban a hálózati eszközök általában fizikailag védve, zárt szobában találhatók, ezért a támadó nehézségekbe ütközik. Ezzel szemben egy védelmi mechanizmusokat nélkülöző vezeték nélküli LAN-hoz való hozzáférés – a rádiós csatorna nyitottsága miatt – triviális feladat a támadó számára. A WEP ezt a triviális feladatot hivatott megnehezíteni. Fontos azonban megjegyezni, hogy a WEP tervezői nem törekedtek „tökéletes” biztonságra, mint ahogy a zárt szoba sem jelent tökéletes védelmet egy Ethernet hub számára.

A tervezők tehát nem tették túl magasra a lécet, ám a WEP még ezt a korlátozott célt sem érte el. Pár évvel a megjelenése után, a kriptográfusok és az IT biztonsági szakemberek súlyos biztonsági hibákat találtak a WEP-ben, s nyilvánvalóvá vált, hogy a WEP nem nyújt megfelelő védelmet. A felfedezést tett követte, és hamarosan megjelentek az Interneten a WEP feltörését automatizáló programok. Válaszul, az IEEE új biztonsági architektúrát

dolgozott ki, melyet a 802.11 szabvány *i* jelzésű kiegészítése tartalmaz. A 802.11i-t a következő fejezetben tárgyaljuk. Ebben a fejezetben a WEP működését és hibáit tekintjük át. Ezt azért tartjuk szükségesnek, mert – bár a WEP-en már túlhaladt a kor – a legtöbb forgalomban levő hálózati eszköz még mindig támogatja a WEP-et. Azok a felhasználók, akik WEP-et használnak, jobb, ha tisztában vannak annak korlátaival.

3.3.1.1. A WEP működése

Vezeték nélküli hálózatok esetében két alapvető biztonsági probléma merül fel. Egyrészt a rádiós csatorna jellege miatt a kommunikáció könnyen lehallgatható. Másrészt – s ez talán fontosabb – a hálózathoz való csatlakozás nem igényel fizikai hozzáférést a hálózati csatlakozóponthoz (Access Point, vagy röviden AP), ezért bárki megpróbálhatja a hálózat szolgáltatásait illegálisan igénybe venni. A WEP az első problémát az üzenetek rejtjelezésével igyekszik megoldani, a második probléma megoldása érdekében, pedig megköveteli a csatlakozni kívánó mobil eszköz (Station, vagy röviden STA) hitelesítését az AP felé.

A hitelesítést egy egyszerű kihívás-válasz alapú protokoll végzi, mely négy üzenet cseréjéből áll. Elsőként a STA jelzi, hogy szeretné hitelesíteni magát (*authenticate request*). Válaszul az AP generál egy véletlen számot, s azt kihívásként elküldi a STA-nak (*authenticate challenge*). A STA rejtjelezi a kihívást, s az eredményt visszaküldi az AP-nak (*authenticate response*). A STA a rejtjelezést egy olyan titkos kulccsal végzi, melyet csak a STA és az AP ismer. Ezért ha az AP sikeresen dekódolja a választ (azaz a dekódolás eredményeként visszakapja saját kihívását), akkor elhiszi, hogy a választ az adott STA állította elő, hiszen csak az ismeri a helyes válasz generálásához szükséges titkos kulcsot. Más szavakkal, a válasz sikeres dekódolása esetén az AP hitelesítette a STA-t, és ennek megfelelően dönthet arról, hogy a csatlakozást engedélyezi vagy sem. A döntésről az AP a protokoll negyedik üzenetében tájékoztatja a STA-t (*authenticate success* vagy *failure*).

Miután a hitelesítés megtörtént, a STA és az AP üzeneteiket rejtjelezve kommunikálnak.

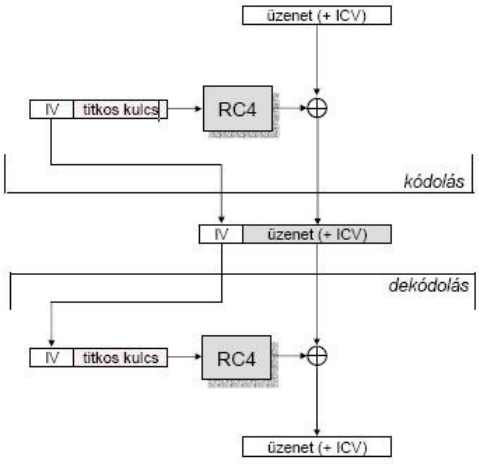
A rejtjelezéshez ugyanazt a titkos kulcsot használják, mint a hitelesítéshez. A WEP rejtjelező algoritmusa az RC4 kulcsfolyam kódoló. A kulcsfolyam kódolók úgy működnek, hogy egy kis méretű, néhány bájtos titkos kulcsból egy hosszú ál-véletlen bájtsorozatot állítanak elő, és ezen sorozat bájtjait XOR-olják az üzenet bájtjaihoz. Ez történik a WEP esetében is. Az *M* üzenet küldője (a STA vagy az AP) a titkos kulccsal inicializálja az RC4 kódolót, majd az RC4 által előállított *K* ál-véletlen bájtsorozatot XOR-olja az üzenethez. Az $M \oplus K$ rejtjelezett

üzenet vevője ugyanazt teszi, mint a küldő: a titkos kulccsal inicializálja az RC4 algoritmust, amely így ugyanazt a *K* ál-véletlen bájtsorozatot állítja elő, amit a rejtjelezéshez használt a küldő. Ezt a rejtjelezett üzenethez XOR-olva – az XOR művelet tulajdonságai miatt – a vevő az eredeti üzenetet kapja vissza: (*M* □ *K*) □ *K* = *M*.

A fent leírtak majdnem megfelelnek a valóságnak, van azonban még valami, amit a WEP rejtjelezés kapcsán meg kell említeni. Könnyen látható, hogy ha a rejtjelezés a fentiek szerint működne, akkor minden üzenethez ugyanazt a *K* ál-véletlen bájtsorozatot XOR-olnánk, hiszen a kódolót minden üzenet elküldése előtt ugyanazzal a titkos kulccsal inicializáljuk. Ez több szempontból is hiba lenne. Tegyük fel például, hogy egy támadó lehallgat két rejtjelezett üzenetet, M_1 □ *K*-t és M_2 □ *K*-t. A két rejtjelezett üzenetet XOR-olva, a támadó a két nyílt üzenet XOR összegét kapja: (M_1 □ *K*) □ (M_2 □ *K*) = M_1 □ M_2.

Ez olyan, mintha az egyik üzenetet a másik üzenettel, mint kulcsfolyammal rejtjeleztük volna. Ám ebben az esetben M_1 és M_2 nem ál-véletlen bájtsorozatok. Valójában tehát M_1□M_2 egy nagyon gyenge rejtjelezés, és a támadó az üzenetek statisztikai tulajdonságait felhasználva könnyen meg tudja fejteni mindkét üzenetet. Az is elképzelhető, hogy a támadó esetleg (részlegesen) ismeri az egyik üzenet tartalmát, s annak segítségével a másik üzenet (részleges) tartalmához azonnal hozzájut.

Ezen problémák elkerülése érdekében, a WEP nem egyszerűen a titkos kulcsot használja a rejtjelezéshez, hanem azt kiegészíti egy IV-nek (*Initialization Vector*) nevezett értékkel, mely üzenetenként változik. A rejtjelezés folyamata tehát a következő: az IV-t és a titkos kulcsot összefűzzük, a kapott értékkel inicializáljuk az RC4 kódolót, mely előállítja az ál-véletlen bájtsorozatot, amit az üzenethez XOR-olunk. A dekódolás folyamata ezzel analóg. Ebből következik, hogy a vevőnek szüksége van a kódolásnál használt IV-re. Ez a rejtjelezett üzenethez fűzve, nyíltan kerül átvitelre. Ez elvileg nem jelent problémát, mert az üzenet dekódolásához csupán az IV ismerete nem elegendő, ahhoz a titkos kulcsot is ismerni kell. A méreteket illetően megemlítjük – s ennek később még lesz jelentősége – hogy az IV 24 bites, a titkos kulcs pedig (általában) 104 bites. A WEP rejtjelezés teljes folyamatát az 4. ábra szemlélteti.



4.ábra: A WEP rejtjelezés folyamata

Az 4. ábra azt is mutatja, hogy a rejtjelezés előtt, a küldő egy integritás-védő ellenőrző összeggel (*Integrity Check Value,* vagy röviden *ICV*) egészíti ki a nyílt üzenetet, melynek célja a szándékos módosítások detektálásának lehetővé tétele a vevő számára. A
WEP esetében az ICV nem más, mint a nyílt üzenetre számolt CRC érték. Mivel azonban a CRC önmagában nem véd a szándékos módosítások ellen (hiszen egy támadó a módosított üzenethez új CRC értéket tud számolni), ezért a WEP a CRC értéket is rejtjelezi. A mögöttes gondolat az, hogy így a támadó nem tudja manipulálni az üzeneteket, hiszen a titkos kulcs hiányában nem tudja a módosított üzenethez tartozó rejtjelezett CRC értéket előállítani. Mint azt alább látni fogjuk, ez a gondolatmenet nem teljesen hibamentes.
Végezetül a WEP kulcsokról szólunk röviden. A szabvány lehetővé teszi, hogy minden
STA-nak saját titkos kulcsa legyen, amit csak az AP-vel oszt meg. Ez azonban megnehezíti a kulcsmenedzsmentet az AP oldalán, mivel ekkor az AP-nek minden STA kulcsát ismernie és gondoznia kell. Ezért a legtöbb implementáció nem támogatja ezt a lehetőséget. A szabvány előír egy ún. default kulcsot is, amit az AP és a hálózathoz tartozó *minden* STA ismer. Eredetileg ezt a kulcsot azon üzenetek védelmére szánták, melyeket az AP többes szórással (broadcast) minden STA-nak el szeretne küldeni. A legtöbb WEP implementáció azonban csak ezt a megoldást támogatja. Így a gyakorlatban, egy adott hálózathoz tartozó eszközök egyetlen közös kulcsot használnak titkos kulcsként. Ezt a kulcsot manuálisan kell telepíteni a mobil eszközökben és az AP-ben. Nyilvánvaló, hogy ez a megoldás csak egy külső támadó

ellen biztosítja a kommunikáció biztonságát; az eszközök (elvileg) dekódolni tudják egymás üzeneteit.

3.3.1.2. A WEP hibái

A WEP tulajdonképpen a rossz protokolltervezés mintapéldája. Az alábbi tömör összefoglalóból látható, hogy lényegében egyetlen kitűzött biztonsági célt sem valósít meg tökéletesen:

Hitelesítés: A WEP hitelesítési eljárásának több problémája is van. Elsőként mindjárt az, hogy a hitelesítés egyirányú, azaz a STA hitelesíti magát az AP felé, ám az AP nem hitelesíti magát a STA felé. Másodszor, a hitelesítés és a rejtjelezés ugyanazzal a titkos kulccsal történik. Ez azért nem kívánatos, mert így a támadó mind a hitelesítési, mind, pedig a rejtjelezési eljárás potenciális gyengeségeit kihasználhatja egy, a titkos kulcs megfejtésére irányuló támadásban. Biztonságosabb lenne, ha minden funkcióhoz külön kulcs tartozna.

A harmadik probléma az, hogy a protokoll csak a hálózathoz történő csatlakozás pillanatában hitelesíti a STA-t. Miután a hitelesítés megtörtént és a STA csatlakozott a hálózathoz, bárki küldhet a STA nevében üzeneteket annak MAC címét használva. Úgy tűnhet, hogy ez annyira nem nagy gond, hiszen a támadó, a titkos kulcs ismeretének hiányában, úgysem tud helyes rejtjelezett üzenetet fabrikálni, amit az AP elfogad. Ám ahogy azt korábban említettük, a gyakorlatban az összes STA egy közös titkos kulcsot használ, s így a támadó megteheti azt, hogy egy STA_1 által küldött – és a támadó által lehallgatott – rejtjelezett üzenetet STA_2 nevében megismétel az AP felé, ezt az AP el fogja fogadni.

A negyedik probléma egy gyöngyszem a protokolltervezési hibák között. Emlékeztetünk arra, hogy a WEP rejtjelezési algoritmusa az RC4 folyamkódoló. Nemcsak az üzeneteket kódolják az RC4 segítségével, hanem a STA ezt használja a hitelesítés során is az AP által küldött kihívás rejtjelezésére. Így a támadó a hitelesítés során küldött üzenetek lehallgatásával könnyen hozzájut a C kihíváshoz és az arra adott $R = C \oplus K$ válaszhoz, melyből $C \oplus R = K$ alapján azonnal megkapja az RC4 algoritmus által generált K ál-véletlen bájtsorozatot. A játéknak ezzel vége, hiszen K segítségével a támadó bármikor, bármilyen kihívásra helyes választ tud generálni a STA nevében (s ezen az IV használata sem segít, mert az IV-t a rejtjelezett üzenet küldője, jelen esetben a támadó választja).

Sőt, mivel a gyakorlatban minden, az adott hálózathoz tartozó eszköz ugyanazt a titkos kulcsot használja, a támadó ezek után bármelyik eszköz nevében csatlakozni tud a hálózathoz. Persze a csatlakozás önmagában még nem elegendő, a támadó használni is szeretné a hálózatot. Ehhez olyan üzeneteket kell fabrikálnia, amit az AP elfogad. A rejtjelezés követelménye miatt ez nem triviális feladat (hiszen magához a titkos kulcshoz még nem jutott hozzá a támadó), de a WEP hibáinak tárháza bőven tartogat még lehetőségeket.

Integritás-védelem: A WEP -ben az üzenetek integritásának védelmét az üzenetekhez csatolt ellenőrző összeg (ICV) hivatott biztosítani. Az ICV nem más, mint az üzenetre számolt CRC érték, mely az üzenettel együtt rejtjelezésre kerül. Formális jelöléseket használva, a rejtjelezett üzenet a következő módon írható fel: $(M \| \mathrm{CRC}(M)) \oplus K$, ahol M a nyílt üzenet, K az RC4 által az IV-ből és a titkos kulcsból előállított ál-véletlen bájtsorozat, CRC(.) jelöli a CRC függvényt, és || jelöli az összefűzés (*konkatenáció*) műveletét.
Ismeretes, hogy a CRC lineáris művelet az XOR-ra nézve, azaz $\mathrm{CRC}(X \oplus Y) = \mathrm{CRC}(X) \oplus \mathrm{CRC}(Y)$. Ezt kihasználva, a támadó a rejtjelezett WEP üzenetek bármely bitjét módosítani tudja (át tudja billenteni), bár magát az üzenetet nem látja. Jelöljük a támadó szándékolt módosításait ΔM-mel. Ekkor a támadó az $((M \oplus \Delta M) \| \mathrm{CRC}(M \oplus \Delta M)) \oplus K$ rejtjelezett üzenetet szeretné előállítani az eredetileg megfigyelt $(M \| \mathrm{CRC}(M)) \oplus K$ rejtjelezett üzenetből. Ehhez egyszerűen $\mathrm{CRC}(\Delta M)$-et kell kiszámolnia, majd a $\Delta M \| \mathrm{CRC}(\Delta M)$ értéket kell az eredeti rejtjelezett üzenethez XOR-olnia. A következő egyszerű levezetés mutatja, hogy ez miért vezet célra:

$((M \| \mathrm{CRC}(M)) \oplus K) \oplus (\Delta M \| \mathrm{CRC}(\Delta M)) =$

$((M \oplus \Delta M) \| (\mathrm{CRC}(M) \oplus \mathrm{CRC}(\Delta M))) \oplus K =$

$((M \oplus \Delta M) \| \mathrm{CRC}(M \oplus \Delta M)) \oplus K$ ahol az utolsó lépésben kihasználtuk a CRC linearitását. Mivel $\mathrm{CRC}(\Delta M)$ kiszámolásához nincs szükség a titkos kulcsra, ezért láthatóan a támadó könnyen tudja manipulálni a WEP üzeneteket, az integritás-védelem és a rejtjelezés ellenére.
Az üzenetfolyam integritásának védelme kapcsán szokás említeni az üzenet visszajátszás detektálását, mint biztonsági követelményt. A WEP esetében ennek vizsgálatával egyszerű dolgunk van, mert a WEP-ben egyáltalán nincs semmilyen mechanizmus, mely az üzenetek visszajátszásának detektálását lehetővé tenné. A tervezők nemes egyszerűséggel erről a biztonsági követelményről megfeledkeztek. A támadó tehát bármely eszköz korábban rögzített üzenetét vissza tudja játszani egy későbbi időpontban, s ezt a WEP nem detektálja. Nyilvánvaló, hogy ez miért gond, ha arra gondolunk, hogy a rögzített üzenet akár egy

bejelentkezési folyamatból is származhat, s például egy felhasználói név/jelszó párt tartalmazhat.

Titkosítás: Mint azt korábban említettük, folyamkódolók használata esetén fontos, hogy minden üzenet más kulccsal legyen rejtjelezve. Ezt a WEP-ben az IV használata biztosítja; sajnos nem teljesen megfelelő módon. A probléma abból adódik, hogy az IV csak 24 bites, ami azt jelenti, hogy kb. 17 millió lehetséges IV van. Egy Wi-Fi eszköz kb. 500 teljes hosszúságú keretet tud forgalmazni egy másodperc alatt, így a teljes IV teret kb. 7 óra leforgása alatt kimeríti. Azaz 7 óránként ismétlődnek az IV értékek, s ezzel az
RC4 által előállított ál-véletlen bájtsorozatok is. A problémát súlyosbítja, hogy a gyakorlatban minden eszköz ugyanazt a titkos kulcsot használja, potenciálisan különböző IV értékekkel, így ha egyszerre *n* eszköz használja a hálózatot, akkor az IV ütközés várható ideje a 7 óra *n*-ed részére csökken. Egy másik súlyosbító tényező, hogy sok WEP implementáció az IV-t nem véletlen értékről indítja, hanem nulláról. Ezért beindítás után a különböző eszközök ugyanazt a nullától induló és egyesével növekvő IV sorozatot használják, legtöbbször ugyanazzal a közös titkos kulccsal. Azaz, a támadónak várakoznia sem kell, azonnal IV ütközésekhez jut.
A WEP teljes összeomlását az RC4 kódoló nem megfelelő használata okozza. Ismeretes, hogy léteznek ún. gyenge RC4 kulcsok, melyekre az a jellemző, hogy belőlük az RC4 algoritmus nem teljesen véletlen bájtsorozatot állít elő. Ha valaki meg tudja figyelni egy gyenge kulcsból előállított bájtsorozat első néhány bájtját, akkor abból következtetni tud a kulcsra. Ezért a szakemberek azt javasolják, hogy az RC4 által előállított bájtsorozat első 256 bájtját mindig dobjuk el, s csak az utána generált bájtokat használjuk a rejtjelezéshez. Ezzel a gyenge kulcsok problémáját meg lehetne oldani. Sajnos a WEP nem így működik. Ráadásul a változó IV érték miatt előbb-utóbb biztosan gyenge kulcsot kap a kódoló, s az IV nyílt átvitele miatt, erről a támadó is tudomást szerezhet. Ezt kihasználva, néhány kriptográfus olyan támadó algoritmust konstruált a WEP ellen, melynek segítségével a teljes 104 bites titkos kulcs néhány millió üzenet lehallgatása után nagy valószínűséggel megfejthető. A WEP minden korábban leírt hibája eltörpül ezen eredmény mellett, ugyanis ezzel a támadással magához a titkos kulcshoz jut hozzá a támadó. Ráadásul a támadás könnyen automatizálható, és néhány „segítőkész” embernek köszönhetően, az Internetről letöltött támadó programok használatával amatőrök által is rutinszerűen végrehajtható.

3.3.2. 802.11i

A WEP hibáit felismerve, az IEEE új biztonsági megoldást dolgozott ki, melyet a 802.11i specifikáció tartalmaz. A WEP-től való megkülönböztetés érdekében, az új koncepciót RSN-nek (*Robust Security Network*) nevezték el. Az RSN-t körültekintőbben tervezték meg, mint a WEP-et. Új módszer került bevezetésre a hitelesítés és a hozzáférés-védelem biztosítására, mely a 802.1X szabvány által definiált modellre épül, az integritás-védelmet és a titkosítást, pedig az AES (*Advanced Encryption Standard*) algoritmusra támaszkodva oldották meg.

Sajnos azonban az új RSN koncepcióra nem lehet egyik napról a másikra áttérni. Ennek az oka, hogy a használatban levő Wi-Fi eszközök az RC4 algoritmust támogató hardver elemekkel vannak felszerelve, és nem támogatják az RSN által előírt AES algoritmust. Ezen pusztán szoftver upgrade-del nem lehet segíteni, új hardverre van szükség, s ez lassítja az RSN elterjedésének folyamatát.

Ezt a problémát az IEEE is felismerte, és egy olyan opcionális protokollt is hozzáadott a 802.11i specifikációhoz, mely továbbra is az RC4 algoritmust használja, és így – szoftver upgrade után – futtatható a régi hardveren, de erősebb, mint a WEP. Ezt a protokollt TKIP-nek (*Temporal Key Integrity Protocol*) nevezik.

A Wi-Fi eszközöket gyártó cégek azonnal adaptálták a TKIP protokollt, hiszen annak segítségével a régi eszközökből álló WEP-es hálózatokat egy csapásra biztonságossá lehetett varázsolni. Meg sem várták, amíg a 802.11i specifikáció a lassú szabványosítási folyamat során végleges állapotba kerül, azonnal kiadták a WPA (Wi-Fi Protected Access) specifikációt, ami a TKIP-re épül. A WPA tehát egy gyártók által támogatott specifikáció, mely az RSN egy azonnal használható részhalmazát tartalmazza. A WPA-ban a hitelesítés, a hozzáférés-védelem, és a kulcsok menedzsmentje megegyezik az RSN-ben használt módszerekkel, a különbség csak az integritás-védelemre és a rejtjelezésre használt algoritmusokban mutatkozik.

A továbbiakban áttekintjük a 802.11i-ben definiált hitelesítési, hozzáférés-védelmi, és kulcsmenedzsment módszereket, melyek tehát megegyeznek az RSN-ben és a WPA-ban.

Ezt követően röviden összefoglaljuk a TKIP (WPA) és az AES-CCMP (RSN) protokollok működését.

3.3.2.1 Hitelesítés és hozzáférés-védelem

A 802.11i-ben a hitelesítés és hozzáférés-védelem modelljét a 802.1x szabványból kölcsönözték. Ezt a szabványt eredetileg vezetékes LAN-ok számára tervezték, de az elvek végül is vezeték nélküli Wi-Fi hálózatokban is ugyanúgy alkalmazhatóak.

A 802.1X modell három résztvevőt különböztet meg a hitelesítés folyamatában: a hitelesítendő felet (*supplicant*), a hitelesítőt (*authenticator*), és a hitelesítő szervert (*authentication server*). A hitelesítendő fél szeretne a hálózat szolgáltatásaihoz hozzáférni, és ennek érdekében szeretné magát hitelesíteni, azaz kilétét bizonyítani. A hitelesítő kontrollálja a hálózathoz történő hozzáférést. A modellben ez úgy történik, hogy a hitelesítő egy ún. port állapotát vezérli. Alapállapotban a port-on adatforgalom nincs engedélyezve, ám sikeres hitelesítés esetén a hitelesítő „bekapcsolja" a port-ot, ezzel engedélyezve a hitelesítendő fél adatforgalmát a port-on keresztül. A hitelesítő szerver az engedélyező szerepet játssza. Tulajdonképpen a hitelesítendő fél hitelesítését nem a hitelesítő, hanem a hitelesítő szerver végzi, és ha a hitelesítés sikeres volt, engedélyezi, hogy a hitelesítő bekapcsolja a port-ot.

Wi-Fi hálózatok esetében a hitelesítendő fél a mobil eszköz, mely szeretne a hálózathoz csatlakozni, a hitelesítő, pedig az AP, mely a hálózathoz történő hozzáférést kontrollálja.

A hitelesítő szerver egy program, mely kisebb hálózatok esetében akár az AP-ben is futhat, nagyobb hálózatoknál azonban tipikusan egy külön erre a célra dedikált hoszt-on futó szerveralkalmazás. Wi-Fi esetében a port nem egy fizikai csatlakozó, hanem egy logikai csatlakozási pont, amit az AP-ben futó szoftver valósít meg.

Vezetékes LAN esetében, a hitelesítendő fél egyszer hitelesíti magát, mikor fizikailag csatlakozik a hálózathoz. További védelmi lépésekre nincsen szükség (legalábbis hozzáférés-védelem tekintetében), hiszen a használatba vett port-ot más úgysem használhatja. Ahhoz ugyanis a hitelesítendő fél és a hitelesítő között létrejött fizikai kapcsolatot kellene megbontani (pl. a hálózati csatlakozót kihúzni egy Ethernet hub-ból).

Ezt a hitelesítő hardvere detektálja és a portot azonnal letiltja. Wi-Fi esetében más a helyzet, mert nincsen fizikai kapcsolat a STA és az AP között. Ezért a 802.11i azzal a követelménnyel egészíti ki a 802.1X modellt, hogy a hitelesítés során létre kell, jöjjön egy titkos kulcs, a STA és az AP között, melyet azok a további kommunikáció kriptográfiai védelmére használhatnak. Ezen kulcs hiányában, egy támadó nem tudja a STA és az AP között kialakult logikai kapcsolatot csalárd módon saját céljainak megvalósítására felhasználni.

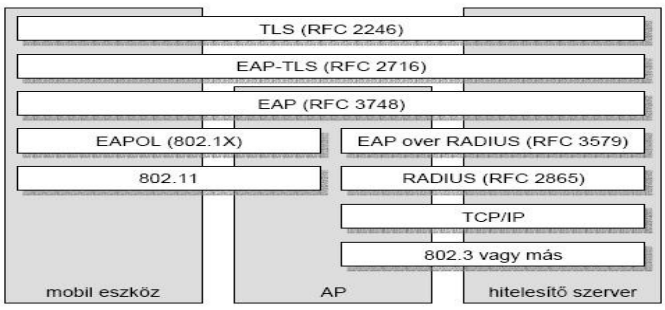
Maga a hitelesítés az EAP (*Extensible Authentication Protocol*) segítségével történik. Az EAP egy igen egyszerű protokoll, aminek az oka, hogy nem maga az EAP végzi a hitelesítést. Az EAP csak egy illesztő-protokoll, amit arra terveztek, hogy tetszőleges hitelesítő protokoll üzeneteit szállítani tudja (ezért „*extensible*"). Egy adott hitelesítő protokoll EAP-ba történő beágyazásának szabályait külön kell specifikálni.

Több elterjedt hitelesítő protokollra létezik már ilyen specifikáció (pl. EAP-TLS, LEAP, PEAP, EAP-SIM).

Négy fajta EAP üzenet létezik: *request*, *response*, *success*, és *failure*. Az EAP request és response üzenetek szállítják a beágyazott hitelesítő protokoll üzeneteit. Az EAP success és a failure speciális üzenetek, melyek segítségével a hitelesítés eredményét lehet jelezni a hitelesítendő fél felé.

Ahogy azt fentebb említettük, a 802.1x modellben, a hitelesítendő fél hitelesítését a hitelesítő szerver végzi. Wi-Fi esetében ez azt jelenti, hogy az EAP protokollt (és az abba beágyazott tényleges hitelesítő protokollt, például a TLS -t) lényegében a mobil eszköz és a hitelesítő szerver futtatják. Az AP csak továbbítja az EAP üzeneteket a mobil eszköz és a hitelesítő szerver között, de nem érti azok tartalmát. Az AP csak az EAP success és failure üzeneteket érti meg, ezeket figyeli, és ha success üzenetet lát, akkor engedélyezi a mobil eszköz csatlakozását a hálózathoz.

Az EAP üzeneteket a mobil eszköz és az AP között a 802.1x-ben definiált EAPOL (*EAP over LAN*) protokoll szállítja. Az AP és a hitelesítő szerver között a WPA a RADIUS protokoll használatát írja elő. A RADIUS -t az RSN opcióként ajánlja, de más alkalmas protokoll használatát is lehetővé teszi a specifikáció. Lényegében tetszőleges protokoll használható, amely az EAP üzenetek szállítására alkalmas. Elterjedtsége miatt azonban várhatóan a legtöbb hálózat RADIUS -t használ majd. Az így kialakuló protokoll architektúrát a 5. ábra szemlélteti.

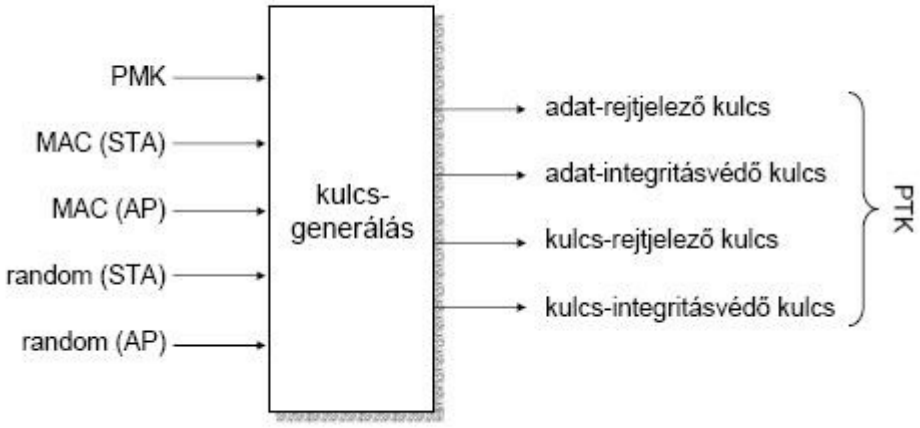


5.ábra: Hitelesítési protokoll-architektúra a 802.11i-ben TLS használata esetén

Ahogy azt korábban említettük, a hitelesítés eredményeként nemcsak a hálózathoz való hozzáférést engedélyezi a hitelesítő szerver, hanem egy titkos kulcs is létrejön, mely a mobil eszköz és az AP további kommunikációját hivatott védeni. Mivel a hitelesítés a mobil eszköz és a szerver között folyik, ezért a protokoll futása után ezt a kulcsot csak a mobil eszköz és a hitelesítő szerver birtokolja, és azt még el kell juttatni az AP -hez. A RADIUS protokoll biztosít erre használható mechanizmust az MS – MPPE – RECV - KEY
RADIUS üzenet-attribútum formájában, mely kifejezetten kulcs-szállítás céljára lett specifikálva. A kulcs rejtjelezett formában kerül átvitelre, ahol a rejtjelezés egy a hitelesítő szerver és az AP között korábban létrehozott (tipikusan manuálisan telepített) kulcs segítségével történik.

3.3.2.2. Kulcsmenedzsment

A hitelesítés során, a mobil eszköz és az AP között létrehozott titkos kulcsot páronkénti mesterkulcsnak (*pairwise master key,* vagy röviden *PMK*) nevezik. Azért „páronkénti”, mert csak az adott mobil eszköz és az AP ismeri (na meg a hitelesítő szerver, de az megbízható entitásnak tekinthető), s azért „mester”, mert ezt a kulcsot nem használják közvetlenül rejtjelezésre, hanem további kulcsokat generálnak belőle. Egészen pontosan a PMK -ból mind a mobil eszköz, mind pedig az AP négy további kulcsot generál: egy adat-rejtjelező kulcsot, egy adat -integritás-védő kulcsot, egy kulcs-rejtjelező kulcsot, és egy kulcs -integritás-védő kulcsot. Ezeket együttesen páronkénti ideiglenes kulcsnak (*Pairwise Transient Key*, vagy röviden *PTK*) nevezik. Megjegyezzük, hogy az AESCCMP protokoll az adatok rejtjelezéséhez és az adatok integritás-védelméhez ugyanazt a kulcsot használja, ezért AES-CCMP használata esetén csak három kulcs generálódik a PMK -ból. A PTK előállításához a PMK-n kívül felhasználják még a két fél (mobil eszköz és AP) MAC címét, és két véletlen számot, melyet a felek generálnak. Ezt a 6. ábra szemlélteti.



6.ábra: A PTK generálása a PMK -ból, a felek MAC címéből, és a véletlen számokból

A véletlen számokat az ún. *négy utas kézfogás* (four way handshake) protokollt használva juttatják el egymáshoz a felek. Ennek a protokollnak további fontos feladata az, hogy segítségével a felek közvetlenül meggyőződjenek arról, hogy a másik fél ismeri a PMK -t.

A négy utas kézfogás protokoll üzeneteit az EAPOL protokoll KEY típusú üzeneteiben juttatják el egymáshoz a felek. Az üzenetek tartalma és a protokoll működése vázlatosan a következő:

1. Első lépésként az AP elküldi az általa generált véletlen számot a mobil eszköznek.

Mikor a mobil eszköz ezt megkapja, rendelkezésére áll minden információ a PTK előállításához. A mobil eszköz tehát kiszámolja az ideiglenes kulcsokat.

2. A mobil eszköz is elküldi az általa generált véletlen számot az AP -nek. Ez az üzenet kriptográfiai integritás-ellenőrző összeggel (*Message Integrity Code*, vagy röviden *MIC*) van ellátva, amit a mobil eszköz a frissen kiszámolt kulcsintegritás- védő kulcs segítségével állít elő. Az üzenet vétele után az AP -nek is rendelkezésére áll minden információ a PTK kiszámításához. Kiszámolja az ideiglenes kulcsokat, majd a kulcs -integritás-védő kulcs segítségével ellenőrzi a MIC -et. Ha az ellenőrzés sikeres, akkor elhiszi, hogy a mobil eszköz ismeri a PMK -t.

3. Az AP is küld egy MIC -et tartalmazó üzenetet a mobil eszköznek, melyben tájékoztatja a mobil eszközt arról, hogy a kulcsokat sikeresen telepítette, és készen áll a további adatforgalom rejtjelezésre. Ez az üzenet tartalmaz továbbá egy kezdeti sorozatszámot. A későbbiekben ettől az értéktől kezdik majd sorszámozni a felek az egymásnak küldött

adatcsomagokat, és a sorszámozás segítségével detektálják a visszajátszásos támadásokat. Az üzenet vétele után a mobil eszköz a kulcs -integritás-védő kulccsal ellenőrzi a MIC -et, és ha az ellenőrzés sikeres, akkor elhiszi, hogy az AP ismeri a PMK -t.

4. Végül a mobil eszköz nyugtázza az AP előző üzenetét, mely egyben azt is jelenti, hogy a mobil eszköz is készen áll a további adatforgalom rejtjelezésére.

A továbbiakban a mobil eszköz és az AP az adat -integritás-védő és az adat-rejtjelező kulccsal védik egymásnak küldött üzeneteiket. Szükség van azonban még olyan kulcsokra is, melyek segítségével az AP többes-szórással küldhet üzeneteket biztonságosan minden mobil eszköz számára. Értelemszerűen, ezeket a kulcsokat az összes mobil eszköznek és az AP -nek is ismernie kell, ezért ezeket együttesen ideiglenes csoportkulcsnak (*Group Transient Key*, vagy röviden *GTK*) nevezik. A GTK egy rejtjelező és egy integritás-védő kulcsot tartalmaz. AES-CCMP esetén a két kulcs ugyanaz, ezért csak egy kulcsból áll a GTK. A GTK -t az AP generálja, és a négy utas kézfogás során létrehozott kulcs-rejtjelező kulcsok segítségével titkosítva juttatja el minden mobil eszközhöz külön-külön.

3.3.3. AES

Az IEEE 802.11i szabvány a TIKP -protokoll mellett tartalmazza a magas szintű titkosítási szabvány (*advanced encryption standard, AES*) protokollt is. Az AES –protokoll alapvetően komolyabb titkosítást tesz lehetővé. Az AES –protokoll az RC4 algoritmus helyett a Rine Dale titkosító algoritmust használja, amely rendkívül erős titkosítási módszer. A legtöbb titkosítással foglalkozó szakember úgy véli, hogy az AES feltörhetetlen. Ráadásul az IEEE 802.11i szabvány az AES –protokollt a TIKP –protokoll felett használható opcióként tartalmazza. Az Egyesült Államok Kereskedelmi Minisztériumának Nemzeti Szabványosítási és Technológiai Intézete (NIST) az elavult Adattitkosítási Szabvány (*Data Encryption Standard, DES*) helyett ma már az AES –titkosítást használja.

Az AES hátránya, hogy sokkal intenzívebb feldolgozási teljesítményt igényel, mint ami a piacon jelenleg kapható hozzáférési pontok biztosítani tudnak. Ezért az AES – protokoll implementálása arra készteti a vállalatokat, hogy az AES –protokoll által elért nagyobb teljesítménnyel szemben támasztott követelményeknek megfelelően fejlesszék tovább meglévő vezeték nélküli lokális hálózati eszközeiket. Problémát jelent továbbá, hogy az AES –protokoll működéséhez koprocesszor, tehát további hardver szükséges. Ez azt jelenti, hogy a vállalatoknak ki kell cserélniük az AES –protokoll implementálásához meglévő hozzáférési pontjaikat és a klienseknél lévő hálózati interfészkártyákat.

3.3.4. WPA (Wi-Fi Protected Access / Wi-fi Védett Elérés)

A **Wi-Fi Protected Access** (**WPA** és **WPA2**) a vezeték nélküli rendszereknek egy a **WEP**-nél biztonságosabb protokollja. A létrehozása azért volt indokolt, mert a kutatók több fontos hiányosságot és hibát találtak az előző rendszerben (**Wired Equivalent Privacy** - vezetékessel egyenértékű biztonságú hálózat - **WEP**). A WPA tartalmazza az IEEE 802.11i szabvány főbb szabályait, és egy átmeneti megoldásnak szánták, amíg a 802.11i szabványt véglegesítik. A WPA úgy lett kialakítva, hogy együttműködjön az összes vezeték nélküli hálózati illesztővel, de az első generációs vezeték nélküli elérés pontokkal nem minden esetben működik. A WPA2 a teljes szabványt tartalmazza, de emiatt nem működik néhány régebbi hálózat kártyával sem. Mindkét megoldás megfelelő biztonságot nyújt, két jelentős problémával:

- Vagy a WPA-nak, vagy WPA2-nek engedélyezettnek kell lennie a WEP-en kívül. De a telepítések és beállítások során inkább a WEP van bekapcsolva alapértelmezettként, mint az elsődleges biztonsági protokoll.
- A "Personal" módban, amit valószínűleg a legtöbben választanak otthon és kishivatali környezetben, a megadandó jelszónak hosszabbnak kell lennie, mint a jellegzetes 6-8 karakter, amit az átlagfelhasználók általában még elfogadhatónak tartanak.

Történet

A WPA-t a Wi-fi Szövetség, egy ipari-kereskedelmi csoport hozta létre, amely a „Wi-Fi” védjegy tulajdonosa és az ilyen védjegyet viselő eszközök hitelesítője.

A WPA az IEEE 802.1x-hitelesített kiszolgálókkal való együttműködésre lett kialakítva, amely különböző kulcsot rendel mindegyik felhasználóhoz; annak ellenére, hogy használható a kevésbé biztonságos "osztott kulcs” – pre-shared key (**PSK**) – módban is, ahol minden felhasználónak ugyanaz a kulcsa a hálózati hozzáféréshez. A WPA tervezésének alapja az IEEE 802.11i szabvány 3. számú vázlata volt.

A Wi-fi Szövetség által létrehozott WPA tette lehetővé a biztonságos vezeték nélküli hálózati eszközök fejlesztésének megkezdését, amíg az IEEE 802.11i-csoport befejezi a szabvány

elkészítését. A Wi-fi Szövetség ekkora már előkészítette a WPA2 szabványt is, ami már az IEEE 802.11i szabvány végleges vázlatára épült, ezért az alkalmazott jelölések a keret mezőkben (Információ Alapfogalmak vagy IE-k) szándékosan különböznek a 802.11i szabványban alkalmazottaktól, hogy elkerüljék az inkompatibilitásokat az egyesített WPA/WPA2 elkészítésekor.

Az adat titkosítás az RC4 adatfolyam-titkosítóval történik, 128-bit kulcs használatával és egy 48-bites induló vektorral (*initialization vector* – IV). A legfontosabb fejlesztés a WPA belül a WEP-hez képest a TKIP bevezetése, amely dinamikusan változtatja az alkalmazott kulcsokat. Ezzel hidalva át a jól ismert kulcs-megszerzéses támadás-t – *key recovery attack* – a WEP-ben.

A hitelesítésben és titkosításban történt fejlesztéseknek köszönhetően a WPA-ban nagymértékben javult a letöltött adatcsomagok integritása. A WEP-ben lévő kevéssé biztonságos „ismétlődő fölös-adat ellenőrzés” (*cyclic redundancy check* – CRC) lehetővé teszi a letöltött csomagok módosítását és a CRC-összeg átírását a WEP kulcs ismerete nélkül is. A jóval biztonságosabb üzenet hitelesítési kód (*Message Authentication Code*, ismertebb nevén MAC, de itt MIC "Üzenet Sértetlenség Kód") a WPA-ban, egy "Michael-algoritmus"nak nevezett eljárás, amely tartalmaz egy keret számlálót, mellyel megelőzi a „replay attacks” (visszajátszásos támadás) végrehajtását.

A kulcsok és az IV-k méretének növekedésével, a jólismert kulcsokkal küldött csomagok számának csökkentésével, és a biztonságosabb üzenet ellenőrzési rendszer hozzáadásával, a WPA-val védett vezeték nélküli hálózatokba sokkal nehezebb a behatolás. A Michael-algoritmus volt a legerősebb védelem amit a WPA tervezői be tudtak építeni a szabványba úgy, hogy az működjön a régebbi hálózat illesztőkkel is. Ám a Michael-algoritmus viszonylagos gyengesége miatt a WPA tartalmaz egy különleges számláló-mechanizmust (CCMP - (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), amely érzékeli a TKIP-törési kísérleteket, és ilyen esetben ideiglenesen blokkolja a kommunikációt a támadó gépével.

WPA 2.0

WPA2-be tehát beépítették a 802.11i. szabvány főbb jellemzőit, főleg a TKIP-t és a Michael algoritmust, továbbá egy új AES-alapú algoritmust, a CCMP-t, mellyel teljesen biztonságossá

tették. Így 2006. március 13-tól kezdődően gyártott minden vezetéknélküli eszköz kötelezően a WPA2 szabvány szerint készült, tehát „Wi-Fi”-jelöléssel ellátott.

Támogatási információk:

- A Microsoft Windows XP WPA2 támogatása hivatalosan 2005. május 1-jétől kezdve létezik. A meghajtó-programok frissítése szükséges lehet.
- Az Apple támogatja a WPA2-t az összes AirPort Extreme Macintoshban, az AirPort Extreme Base Station-ökben, és a AirPort Expressz-ekben. A szükséges Firmware-frissítést tartalmazza az AirPort 4.2, 2005. július 14-én kibocsátott változata.

Biztonság osztott kulcs módban

Az osztott (*Pre-shared*) kulcs módot (PSK, más néven „*Personal*” mód) azon otthoni és kisirodai felhasználóknak fejlesztették ki, akik nem tudnak megengedni (ára és bonyolultsága miatt) egy dedikált 802.1x kiszolgálót. Mindegyik felhasználónak kell egy „*passphrase*” (jelmondat – azaz egy összetett jelszó) a hálózat eléréséhez. A jelszónak 8-63 darab nyomtatható ASCII karakterből vagy 64 darab hexadecimális számjegyből (256 bit) kell állnia. (IEEE Std. 802.11i-2004, Annex H.4.1) Ha csak ASCII karaktereket használunk, egy hash-funkció csökkenti az 504 bites hosszúságot (63 karakter * 8 bit/karakter) 256 bites hosszra (amelyet az SSID is használ). A jelszó a felhasználó számítógépén tárolódik, amivel a legtöbb operációs rendszer alatt elkerülhető az ismételt begépelés. A jelszót a Wi-fi elérési pontban is tárolni kell.

Megnövelhető a biztonság egy PBKDF2 kulcs-generálási funkció használatával. Természetesen a legtöbb felhasználó tipikusan gyenge jelszót ad meg, kitéve a hálózatot a jelszótöréses támadásnak. Ez legjobban úgy kerülhető el, ha a használt jelszó legalább „5-dobásos”, 14 teljesen véletlenszerű karakterből áll WPA és WPA2 alkalmazása mellett.

A maximális WPA-PSK védelemhez (256 bit) olyan kulcs kell, ami 54 véletlenszerű karaktert, vagy 39 véletlenszerű ASCII karaktert tartalmaz.

Néhány lapkagyártó úgy próbálja meg kiküszöbölni a gyenge jelszavak megadását, hogy egy új Wi-fi illesztő, vagy hálózati eszköz telepítése során, egy program vagy hardver interfész által automatikusan létrehoz egy megfelelő erősségű jelszót. Ez a módszer úgy működik, hogy a felhasználó által lenyomott billentyűhöz (Broadcom SecureEasySetup és Buffalo AirStation

One-Touch Secure System) hozzáadódik a program által (pl. Atheros JumpStart) generált kifejezés. Az Wi-fi Szövetség most dolgozik az eljárás szabványosításán, hogy a védett beállításnak (Protected Setup, régebben Easy Config) részévé válhasson.

EAP típusok WPA és WPA2 alatt

A Wi-fi szövetség bejelentette hogy a szabványba illeszti az alább felsorolt EAP (Extensible Authentication Protocol – bővíthető hitelesítési protokoll) típusokat a WPA- és WPA2-Enterprise hitelesítési programjának keretében. Ez igazolja, hogy a WPA-Enterprise-ként jelölt eszközök biztosan együttműködnek egymással. Azelőtt, csak az EAP-TLS-t (Transport Layer Security – vivőréteg biztonság) hitelesítette a Wi-fi szövetség.

A hitelesítési programba kapcsolt EAP típusok:

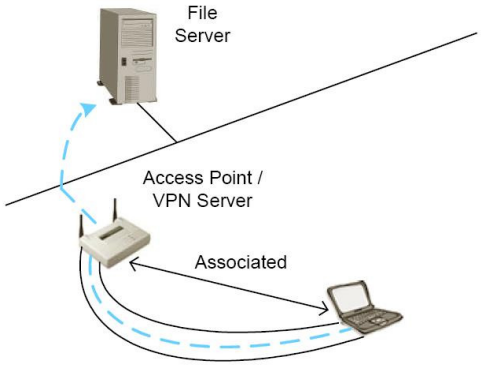
- EAP-TLS (azelőtt tesztelt)
- EAP-TTLS/Mschapv2
- Peapv0/Eap-mschapv2
- Peapv1/EAP-GTC
- EAP-SIM
- EAP-LEAP

Az egyéb, céges rendszerek számára készített speciális 802.1x kliens és szerver Wi-Fi eszközök ezektől eltérő EAP típusokat is támogathatnak.

Ez a hitelesítési program még csak egy kísérlet a népszerű EAP típusok együttműködésének megteremtésére, ezek vélhető inkompatibilitása jelenleg egy, azon problémák között, amiért sok esetben tartózkodnak a 802.1x bevezetésétől heterogén hálózatokban.

3.3.5. Virtuális magánhálózatok

Nyilvános helyen – például repülőtéren vagy szállodában is – megforduló, vezeték nélküli felhasználóknak érdemes megfontolnia a virtuális magánhálózat (*virtual private network, VPN*) használatát. A virtuális magánhálózat igényel ugyan némi hozzáértést, a végpontok között történő titkosításnak azonban hatékony eszköze lehet. A virtuális magánhálózat – mivel az eltérő hálózati kapcsolódási szinteknél magasabb szinten működik – akkor is jól használható, amikor a kliensek különböző típusú vezeték nélküli hálózatban barangolnak.



7.ábra. A virtuális magánhálózat

3.3.6. MAC –szűrők

Egyes vezeték nélküli bázisállomások lehetőségét biztosítanak közeghozzáférés-vezérlési (MAC) szűrésre. A MAC -szűrés implementálásához a hozzáférési pont minden érkező keretben megvizsgálja a forrás MAC –címét. A hozzáférési pont minden olyan keretet visszautasít, amely nem a rendszeradminisztrátor által beprogramozott speciális listán található MAC –címet tartalmazza. A MAC –szűrés ezzel a hitelesítés egyszerű változatát valósítja meg.

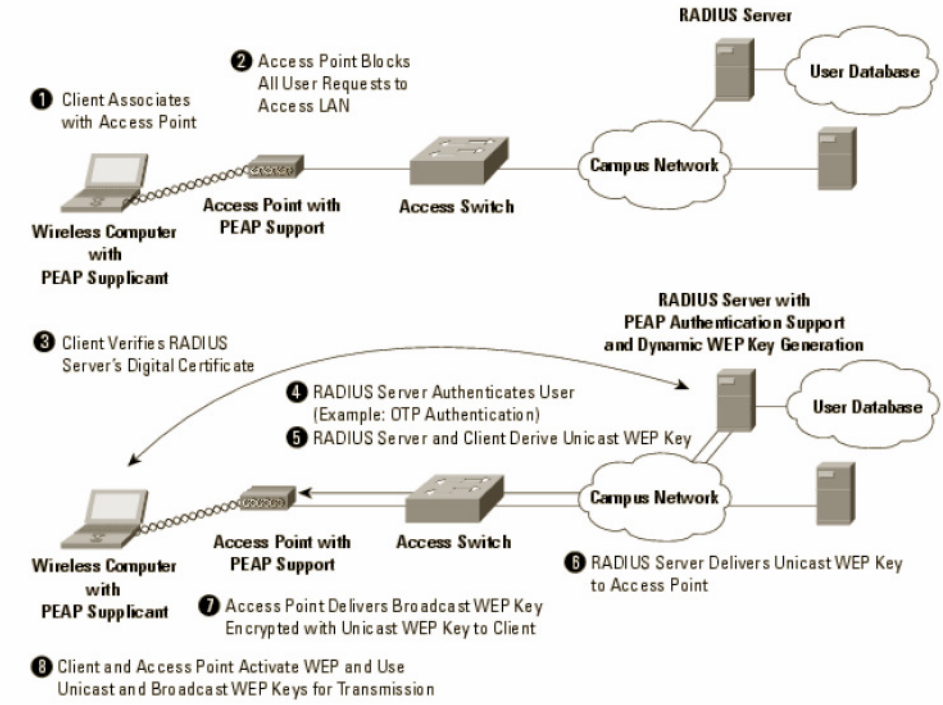
A MAC –szűrésnek azonban van néhány gyenge pontja. Például a WEP –titkosítás a keret MAC –címmezőjét nem titkosítja, ezért a hacker le tudja hallgatni a keretek adását és így érvényes MAC –címekhez juthat. Ezt követően a hacker egy szabadon beszerezhető szoftver segítségével, a MAC –címekhez tartozó rádiófrekvenciás hálózati interfészkártyákat úgy átprogramozhatja, hogy azok MAC –címe megfeleljen egy érvényes MAC –címnek. Ily módon a hacker valódi felhasználónak álcázhatja magát és megtéveszteti a hozzáférési pontot, amikor a jogos felhasználó nem tartózkodik a hálózatban.

Ha a rendszerben több felhasználó van, a MAC –szűrés kezelése meglehetősen unalmas. A rendszeradminisztrátornak az összes felhasználói MAC –címet egy táblázatba kell begépelnie, majd megfelelő módosításokat kell végrehajtania, amikor új felhasználó lép a rendszerbe. Ha

például egy másik vállalati részlegtől érkező alkalmazottnak látogatása idejére hozzáférést kell biztosítani a vezeték nélküli lokális hálózathoz, a rendszeradminisztrátornak meg kell határoznia, és a rendszerbe kell programoznia a MAC –címet, mielőtt a látogató hozzá kívánna férni a hálózathoz. A MAC –címszűrés kisebb otthoni vagy irodai alkalmazásoknál jó megoldás lehet, a kézi módszer miatt azonban a vállalati vezeték nélküli hálózatok rendszeradminisztrátorai nem nagyon kedvelik.

3.3.7. Hitelesítő szerver – RADIUS (Remote Authentication of Dial-In User Service)

A RADIUS szervert eredetileg Internet Szolgáltatók használták ügyfeleik jelszavas hitelesítésére, a szolgáltató hálózatába történő belépés előtt. A 802.1X keretszabvány nem írja elő a háttérben működő hitelesítő szerver típusát, de a RADIUS tekinthető alapértelmezett autentikációs szervernek 802.1X környezetben.



8.ábra Az ábrán az autentikációs folyamat sémája látható

3.3.8.SecureMyWiFi RADIUS szolgáltatás

A SecureMyWiFi egy Interneten elérhető RADIUS (Remote Authentication Dial-In User Service) szolgáltatás.
A szolgáltatás lényege, hogy nem kell üzemeltessünk amúgy is bonyolult beállításokat követelő RADIUS szervert, (pl.: FreeRADIUS) hanem némi pénzösszeg fejében ezt elvégzi helyettünk a SecureMyWiFi ! Mégpedig úgy, hogy a szolgáltatás weboldalán egy regisztrációs folyamaton keresztül kapunk egy felhasználói név/jelszó párost és egy biztonságosan beállított RADIUS szerver IP címet (vagy domain nevet) melyet aztán egy WiFi -s routernek vagy AP -nak megadva működik is RADIUS szolgáltatásunk.
A szolgáltatás ára meglepően alacsony! Az alap szolgáltatás éves díja 29$ mely 1db AP + 5db hozzá kapcsolódó felhasználó "biztonságosabbá tételét" tartalmazza. További AP-k 10$-os áron, felhasználók (max. 25) pedig 1$-os plusz költséggel adhatók a rendszerhez.
Sajnos jelenleg kevés eszközt támogat a szolgáltatás, de az ígéretek szerint hamarosan a cég közzétesz egy listát, mely részletesen tartalmazza majd a támogatott eszközök pontos típusait.
A dokumentáció szerint minden WPA/WPA2-Enetrprise - vagy Enterprise helyett RADIUS jelzésű eszközt támogat a rendszer. Azt hogy saját eszközünk támogatja-e ezt a funkciót erről a wifialliance.org weboldalon győződhetünk meg.

3.4. Biztonsági rendszabályok

Ahhoz, hogy egy vezeték nélküli hálózatot biztonságossá tehessünk, első lépésként hatékony rendszabályokat kell kidolgoznunk, illetve kényszerítő eljárásokat alkalmaznunk erre vonatkozóan. A biztonsággal szembeni elvárásokat alaposan ki kell elemeznünk, és megfelelő szintű védelmet létrehozásáról kell gondoskodnunk. Például minden vezeték nélküli hálózatban kötelező jelleggel alkalmaznunk kell valamilyen titkosító algoritmust. A WEP jól használható lakásban és kisebb irodai alkalmazásoknál, a vállalati alkalmazásoknál azonban ennél jobb módszereket, például a WPA -t kell használni. A hatékony kölcsönös hitelesítési eljárás, mint amilyen a LEAP vagy az EAP-TLS, szintén fontos a vállalati alkalmazások számára.
Amint létrehoztunk egy vezeték nélküli hálózatot, biztonsági értékelést kell végrehajtani, hogy megbizonyosodjunk, a hálózatunk eleget tesz a biztonsági követelményeknek, előírásoknak. Nem jó stratégia teljes mértékben megbízni a rendszerterven! Akkor járunk el körültekintően, ha teszteket futtatunk annak érdekében, hogy megbizonyosodjunk arról, hogy

a hálózatot kellő képen megerősítettünk, és így megakadályozza illetéktelen személyek hozzáférését az erőforrásainkhoz.

A vállalatoknak szabályszerű és rendszeres biztonsági ellenőrzést kell elvégezniük ahhoz, hogy az esetleges módosítások a rendszerben, nem tették-e azt sebezhetőbbé, mint amelyen a változtatások előtt volt. A kisebb kockázatú rendszereknél az évenkénti egy ellenőrzés elegendő lehet, de az erősen veszélyeztetett információkat (pl. pénzintézetek, postai adatok esetében) negyedévente, vagy ennél is gyakrabban kell ellenőrizni.

3.4.1. A saját, már meglévő biztonsági rendszabályok ellenőrzése

Ez tájékoztatást ad arról, hogy a vállalat teljesíti-e a saját előírásait. Ezen felül, itt nyílik lehetőség arra is, hogy a rendszabályok értékelésén túlmenően, a módosításukra vonatkozó megfelelő javaslatokat is megtegyék az ebben érdekeltek. Érdemes például azt is megvizsgálni, hogy az elégedetlen alkalmazottak, hozzáférhetnek-e a vállalat erőforrásaihoz esetleges károkozás céljából is! A rendszabályok előírhatják, hogy a bázisállomások beszerzése és telepítése előtt a konfigurációt minden alkalmazottnak egyeztetnie kell a vállalat információtechnológiai osztályával. Fontos tehát, hogy minden bázisállomásnak olyan konfigurációs beállításai legyenek, amelyek megfelelnek a rendszabályoknak, és megfelelő szintű biztonságot nyújtanak. Ezen kívül, arról is meg kell győződni, hogy az alkalmazottak elsajátították-e a biztonsági rendszabályokat.

3.4.2. A jelenleg működő rendszer áttekintése

Meg kell vizsgálnunk, hogy vannak-e olyan tervezési hibák amelyek támadási felületet jelenthetnek. A lehető legalaposabban ismerkedjünk meg a meglévő terméktámogatási eszközökkel és a lehetséges problémák helyét azonosító eljárásokkal. A legtöbb vállalat például a vezetékes Ethernet –gerinchálózaton keresztül konfigurálja a bázisállomásokat. Ennél a folyamatnál az adott bázisállomással létesítendő összeköttetés megnyitása céljából továbbított jelszavakat titkosítás nélkül juttatják el a vezetékes hálózatba. Tehát az Ethernet –hálózathoz monitorozó berendezéssel kapcsolódó hacker könnyen elfoghatja a jelszavakat és átkonfigurálhatja a bázisállomást.

A felhasználó kikérdezése is fontos momentum lehet. Megtudhatjuk ezáltal, hogy tisztában vannak-e azzal, hogy a vezeték nélküli komponensek beszerzése, és telepítése során együtt kell működnie a megfelelő osztállyal. Ha van is ilyen előírás, ne bízzunk abban, hogy mindenki ismeri. Nehezen leküzdhető és a hálózat biztonságát komolyan veszélyeztető

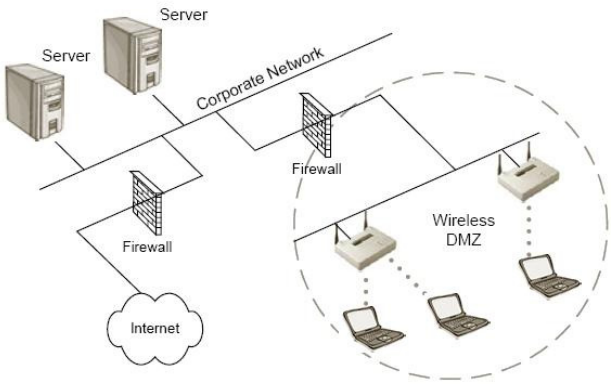
probléma léphet fel, ha az alkalmazott az irodájában személyes bázisállomást is üzemeltet. Ugyanis ezek a bázisállomások az esetek többségében nem felelnek meg a biztonsági rendszabályoknak, és nyitott, nem biztonságos bemeneti porttal csatlakoznak a vállalati hálózathoz. Az engedély nélkül használt bázisállomások felderítése szintén az értékelés részét képezik. A legtöbb vállalatvezető meglepődne, ha megtudná, hogy hány ilyen bázisállomása van. A csaló bázisállomások felderítésének módszere lehet, hogy lehallgató készülékkel végigjárjuk az épületet.

3.4.3. Ajánlott fejlesztések

Miután a gyenge pontokat megtaláltuk, keressük meg és dokumentáljuk azokat a módszereket, amelyekkel megoldhatjuk a problémákat. Szigorítsuk a rendszabályokat a vállalat védelmének érdekekében.
Nézzünk meg néhány intézkedést a magasabb fokú védelem nevében.

3.4.3.1. A vezeték nélküli felhasználók tűzfalon kívüli elhelyezése

Érdemes vezeték nélküli demilitarizált zónát (DMZ) létrehozni úgy, hogy tűzfalat létesítünk a vezeték nélküli hálózat és a vállalati hálózat között.



9.ábra. Vezeték nélküli demilitarizált zóna

Ennél a megoldásnál minden klienseszközt olyan virtuális magánhálózattal látunk el, amelyet a védett hálózat elfogad. A hackernek a vállalati erőforrásokhoz való hozzáféréshez helyesen konfigurált virtuális magánhálózattal kell rendelkeznie ami igen nehéz feladat. Hátránya ennek a módszernek – miszerint minden felhasználót virtuális magánhálózattal látunk el – hogy az ilyen rendszer nehezen kezelhető és időnként a teljesítménye is csökkenhet. Ezért a

virtuális magánhálózatok alkalmazását elsősorban akkor vegyük fontolóra, ha a felhasználók várhatóan nyilvános területekre is kiléphetnek.

3.4.3.2. Rendszerprogramok frissítése

A forgalmazók a bázisállomásokban és a rádiófrekvenciás hálózati interfészkártyákban futó rendszerprogramokhoz gyakran implementálnak olyan javítóprogramokat (patch), amelyek megszüntetik a biztonsági problémákat. Tegyük szokássá annak ellenőrzését, hogy jelentek-e meg ilyen javító csomagok, és ha igen ezek telepítése magától értetődő legyen. Már a vásárláskor érdemes azt is figyelembe venni, hogy az általunk megvenni kívánt eszközhöz könnyen beszerezhetőek-e a szoftverfrissítések.

3.4.3.3. Bázisállomások fizikai rögzítése

Vannak olyan bázisállomások, amelyek a „reset” gomb megnyomásával visszalépnek a semmilyen biztonságról nem gondoskodó gyári alapbeállításukhoz. Az ilyen eszközök sebezhető belépési pontot jelenthetnek, tehát gondoskodni kell a bázisállomás hardvere számára megfelelő fizikai biztonságról, magyarul ne helyezzük olyan asztalra az irodában, amely könnyen megközelíthető, ehelyett szerelhetjük álmennyezet fölé, nem látható helyre. Üzemszünet esetén, vagy ha a felhasználóknak nincs szüksége a bázisállomásra, akkor kapcsoljuk ki, ezzel is rövidítve az illetéktelen felhasználók számára a hozzáférési időt.

3.4.3.4. Bonyolult jelszavak bázisállomásokhoz rendelése

Ne használjuk a bázisállomások alapértelmezett jelszavait! Az alapértelmezett jelszavak jól ismertek, tehát a bázisállomás konfigurációs paramétereit saját céljai érdekében bárki megváltoztathatja. Használjunk inkább nehezen kitalálható jelszavakat. Jó ötlet például a nagybetűk és kisbetűk együttes alkalmazása, illetve a különleges karakterek „bevetése”. Gondoskodni kell a jelszavak rendszeres megváltoztatásáról is. Győződjünk meg arról, hogy jelszavainkat a hálózaton történő továbbítás előtt feltétlenül titkosítsuk!

3.4.3.5. A rádióhullámok terjedésének csökkentése

Irányított antennák lehetőséget adnak arra, hogy a rádióhullámok terjedését olyan területekre korlátozzuk, ahol a hackerek fizikailag nem férhetnek hozzájuk. Ha például a vezeték nélküli hálózat antennája olyan erősítési tényezővel és orientációval rendelkezik, amellyel a rádióhullámok épületből való kilépése csökkenthető, ez nem csak a fedettséget optimalizálja,

hanem minimalizálja annak esélyét, hogy az illetéktelen behatoló a továbbított felhasználói jelekbe belehallgasson, vagy egy hozzáférési ponton keresztül a vállalati hálózathoz csatlakozzon.

3.4.3.6. Személyi tűzfalak létesítése

Lényeges, hogy minden felhasználó tiltsa meg a fájlmegosztást a mappáiban, és mindenki használjon személyi tűzfalat, ezzel is kiaknázva újabb támadási felületek meglétét. Ennek akkor van kiemelt jelentősége, ha a felhasználó nyilvános helyen is használja a hálózatot.

Hozzáférés ellenőrzés (Access Control) A hálózatunkhoz csatlakozó gépek IP címeinek és különböző (pl. web, FTP, email hozzáférés) szabályok, illetve időzítés megadásával korlátozhatjuk az internet hozzáférést. Jó példa erre egy irodai felhasználás esetén, hogy az említett szolgáltatásokat csak munkaidőben lehessen elérni számítógépeinkről alkalmazottaink egy csoportjának.

Internet cím szűrés (URL Blocking) Az itt felsorolt Internet címek elérését a router nem engedélyezi hálózatunkhoz kapcsolódó eszközeink számára.

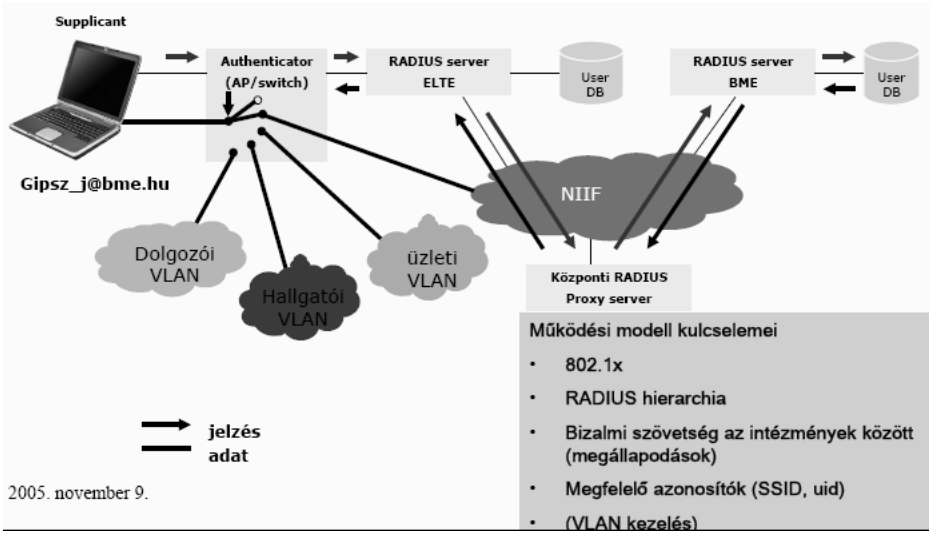
Betörés figyelés (Intrusion Detection) Különböző szokásos betörési kísérletek elhárítását szolgálja ez a funkció, mint például az IP Spoofing, Land Attack, Ping of Death, UDP Port Loopback, stb. Ezek ismertetésébe most nem mélyedünk el, azonban annyit érdemes megemlíteni, hogy bizonyos internetes szoftverek működését (pl. Skype) igen csak meg tudja nehezíteni néhány beállítás. Használata ennek ellenére javasolt.

3.5.Eduroam

Az Eduroam (Education Roaming) szolgáltatást jelent a mobilitás és a kutatói környezet megvalósításához. AutN infrastruktúra, mely már meg lévő eszközökre, illetve megoldásokra épül. Bizalmi szövetségen alapuló autentikációs keretrendszer, amely a kutató hálózatokhoz hasonlóan hierarchikusan épül fel. Kutatói hálózati kezdeményezés (TF- Mobility).

Hozzávetőlegesen 20 ország és körülbelül 400 intézmény csatlakozik hozzá. Felhasználók tulajdon képen, a csatlakozó intézmények dolgozói, hallgatói. Igen dinamikus fejlődés jellemzi, egyre többen tervezik a csatlakozást. Természetesen a globális lefedettség a cél.

Működési modell:



10.ábra A működési modell

Főbb követelmények:

Szükséges megállapodás az NREN és az Eduroam szövetség között, továbbá az NREN és a csatlakozó intézménynek is megállapodást kell aláírniuk. Mindkét megállapodásban a következő főbb kitételek találhatóak:

- A fogadó intézmény AUP -jának betartása,
- Authentikációs szerver működtetése,
- Biztonságos authentikáció (titkosított csatorna),
- Információ biztosítása a szolgáltatásról,
- Tájékoztatás a biztonsági szintről,
- Oktatást és supportot az anyaintézmény nyújtja,
- Authentikációs folyamat és hálózatelérés loggolása,
- Biztonsági események jelentése.

3.5.1. Csatlakozás a Debreceni Egyetem Eduroam Wi-Fi hálózatához

Az Egyetemünkön működő Eduroam vezeték nélküli hálózat használatához szükséges konfigurációs lépések a következők:

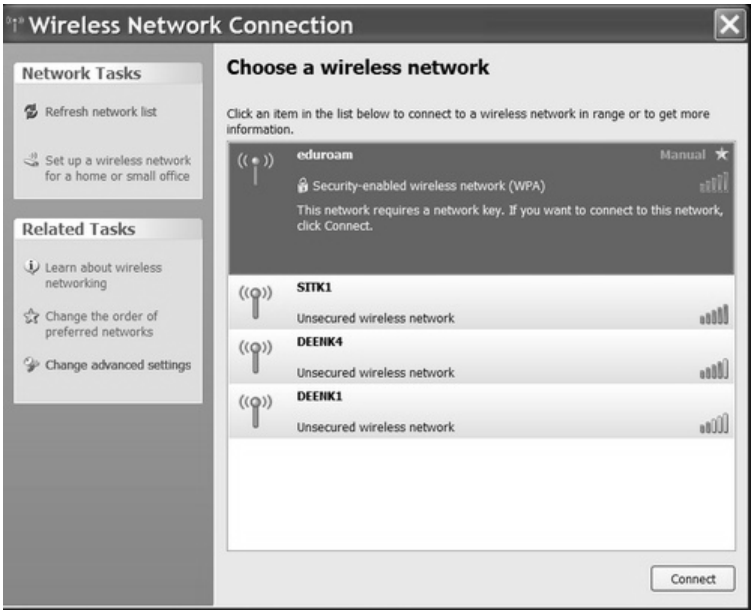
1. Először is létre kell hozni egy hálózati azonosítót a https://directory.unideb.hu/adataim oldalon.
2. Ugyanezen az oldalon a *Hálózati adatok* beállításánál a *WiFi hálózati elérés* menüpontban a hozzáférés aktiválása.

Rendszerkövetelmények

- Vezetéknélküli hálózati adapter, támogatott szabványok: IEEE 802.11b/g, az Élettudományi Épületben ezek mellett 802.11a is használható.
- WPA vagy WPA2 kompatibilitás (autentikáció: PEAP-MSCHAPv2, titkosítás: TKIP, AES).
- Windows XP SP2, Vista
- Linux kliens és WPA Supplicant.
- Regisztráció: https://directory.unideb.hu/adataim

Wireless hálózat konfigurálása Windows XP-ben

1. Vezetéknélküli kapcsolatok



11.ábra

A ***Change advanced settings*** menüpontra kattintva elérhetjük a vezetéknélküli hálózatok beállításait.

Itt válasszuk ki azt a hálózatot, melyhez csatlakozni szeretnénk - a mi esetünkben ez az eduroam - majd kattintsunk a ***Properties/Tulajdonságok*** gombra

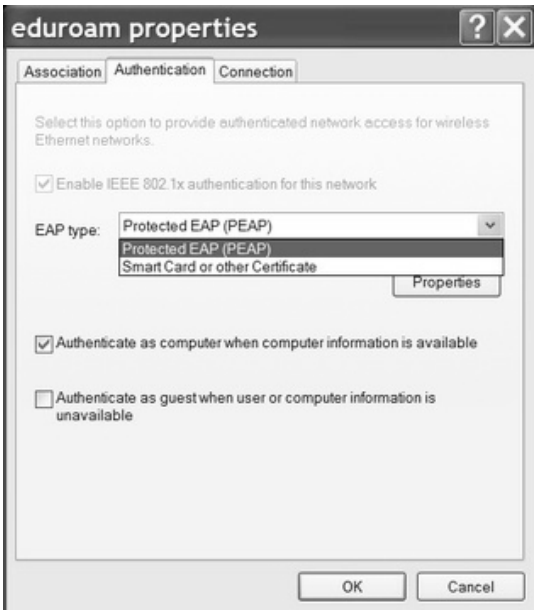
12.ábra **13.ábra**

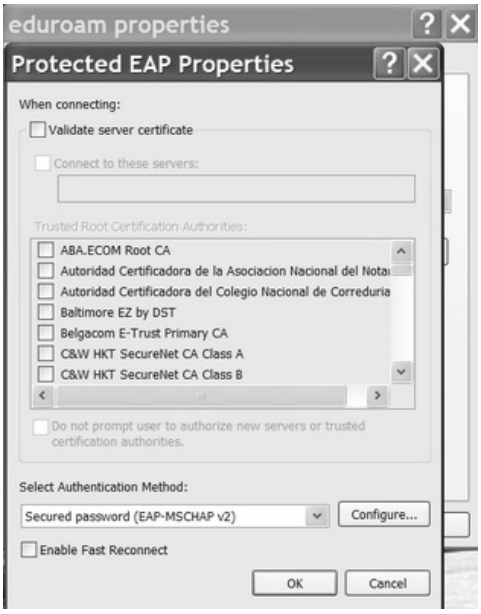
Network Authentication/Hálózati hitelesítés: WPA (13. ábra)

Data encryption/Adattitkosítás: TKIP vagy AES - a kártya/driver képességeinek megfelelően (13. ábra)

EAP type/Autentikációs protokoll: Protected EAP (PEAP):

A PEAP tulajdonságainak módosítása:

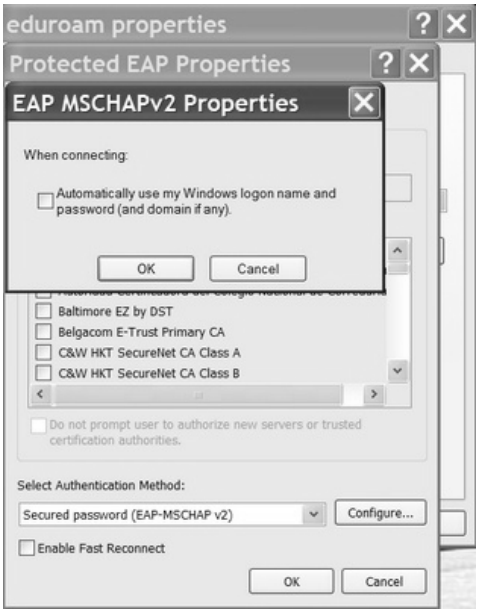




14.ábra **15.ábra**

A ***Validate server certificate*** opció ne legyen kiválasztva!

Fontos, hogy a kliensprogram ne a Windows felhasználói névvel próbáljon hitelesíteni minket, ezért az *Automatikus Windows logon name* opció ne legyen kiválasztva!



16.ábra

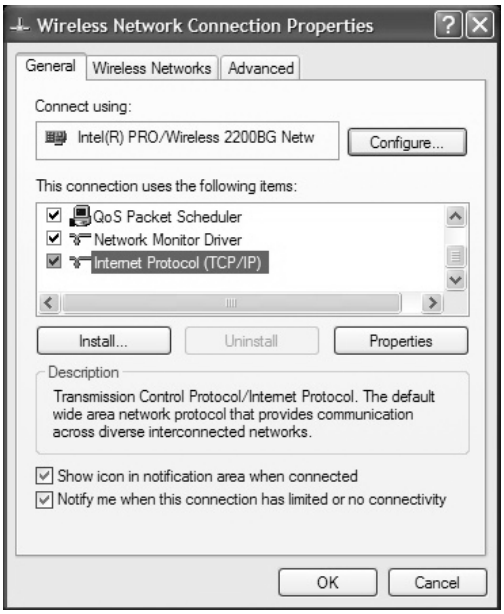
Miután módosítottuk a beállításokat, csatlakozhatunk a kívánt hálózathoz a ***Wireless Network Connection*** ablakban. Az egyetemi vezeték nélküli hálózatok védett hálózatok, így kapcsolódáskor felhasználói név és jelszó megadásával hitelesítenünk kell magunkat.

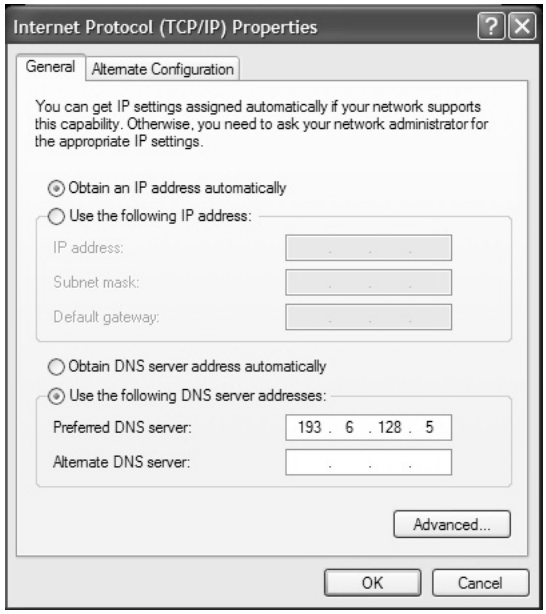
Bejelentkezéskor a felhasználói nevet az alábbi formátumban kell megadni: **felhasználóinév@unideb.hu**

Mivel a Windows XP tárolja az itt megadott felhasználói adatokat, ezért a következő kapcsolódáskor automatikusan hitelesít minket a rendszer.

2. A vezetéknélküli adapter TCP/IP beállításai

Miután sikeresen csatlakoztunk az egyetemi WiFi hálózathoz, a kliensgép automatikusan kap IP címet (a megfelelő alhálózatból DHCP szerver osztja ki a címeket; a kliens gép megkapja a subnet maszkot, valamint az alapértelmezett átjáró és a DNS IP címét is). Ehhez a kliens gépen a wireless hálózati kártyához tartozó TCP/IP tulajdonságainál az alábbi beállítást kell elvégezni:



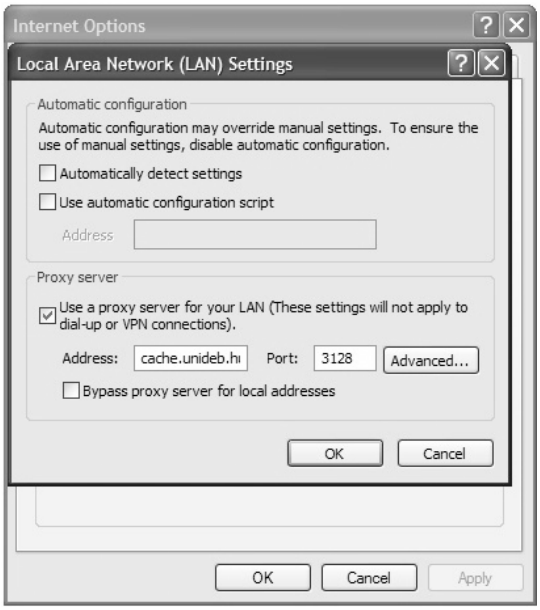


17.ábra **18.ábra**

3. A böngésző proxy beállításai

A DHCP szerver privát IP tartományból oszt címeket, ezért Web-böngészéshez proxy szervert kell beállítani.

Eszközök/Internet beállítások/Kapcsolatok/LAN beállítások:



19.ábra **20.ábra**

Cím: cache.unideb.hu Port: 3128

3.6. Történelmi áttekintés

Befejezés képen egy kis történelmi összefoglaló arról, hogyan alakult ki a vezeték nélküli hálózat mai szabványa az elmúlt évtizedek alatt.

1942

A zeneszerző / zongoraművész George Antheil és a színésznő Hedy Lamarr szabadalmaztatja egy frekvencia-ugrásos rádiótitkosító (később "szórt-spektrumú"-nak elnevezett) technikát, majd felajánlotta az amerikai tengerészetnek (U.S. Navy), amely befogadta, de még nem találta használhatónak a II. Világháborúban.

1958

Az amerikai tengerészet kifejleszti az első rádió kommunikációs chipet, amely ezen a technológián alapult.

1985

Az amerikai tengerészet elérhetővé teszi a civil szféra számára a technológiát.

1989

Az FCC (Federal Communications Commission - Amerikai Hírközlési Hatóság) engedélyezi a technológiát három szabad rádió sávra.

1990

Az IEEE megkezdi a vezeték nélküli kapcsolat szabványának kidolgozását az ISM (Industrial, Scientific and Medical - Ipari, Tudományos és Orvosi) spektrumban.

1997

Az IEEE ratifikálja a 802.11 "over-the-air vezeték nélküli kliensek és alap-állomások közötti interfész" -t, amely még nem garantálta a szabványok együttműködését. Az FCC engedélyezi egy negyedik frekvencia sáv használatát is.

1999

Az IEEE ratifikálja a 802.11b és 802.11a szabványt. Megalakul a WECA (Wireless Ethernet Compatibility Alliance - vezeték nélküli Ethernet Kompatibilitás Szervezet) a 802.11 szabványban való együttműködés összehangolására, megindítva globális elterjedését. Megkezdődik a 802.11b szabványú termékek kiszállítása.

2000

A Microsoft kiadja a Windows 2000 -ret WLAN sniffer képességgel felvértezve. A WECA elindítja Wi-Fi hitelesítő programját a 802.11b szabványt támogató termékekre. A Carlson Hotels Worldwide (a Country Inns & Suites, a Radisson Hotels és a Regent International Hotels tulajdonosa) bejelenti vezeték nélküli szolgáltatását.

2001

A Starbucks is elindítja vezeték nélküli hotspot szolgáltatását. Scott Fluhrer, Itsik Mantin, és Adi Shamir kutatók bejelentik, hogy a WEP (Wired Equivalent Privacy - Vezetékessel Egyenértékű Titkosítás), a 802.11 biztonsági megoldása bizonyítottan megbízhatatlannak minősült. A 802.11a szabványú termékek megjelennek a piacon.

2002

A Lucent Technologies bemutatja, hogyan képesek a felhasználók a nélkül váltani a Wi-Fi és 3G hálózatok között, hogy megszakadna Internet kapcsolatuk. A WECA új szervezetté alakul, Wi-Fi Alliance (WFA, Wi-Fi szövetség) néven, elindítja a 802.11a hitelesítő tesztjeit illetve

és bejelenti a WPA (Wi-Fi Protected Access, Wi-Fi védett hozzáférés) biztonsági módszert a WEP leváltására.

2003

A WFA elindítja Wi-Fi ZONE programját publikus hotspotok hitelesítésére. Az Intel bemutatja a Centrino technológiát, amely hardveresen támogatja a vezeték nélküli kapcsolatokat. A McDonald's tíz hotspot-ot telepít Manhattan-ben és további 300-at ígér az év végéig. Megjelennek az első, még nem véglegesített 802.11g szabványt támogató termékek. A WFA hitelesíti az első WPA-t támogató termékeket. Ekkor már több, mint 40 millió 802.11 szabványt támogató terméket adnak el világszerte, illetve megjelennek az első 802.11a és 802.11g szabványt egyszerre támogató termékek is. A Verzion 150 Wi-Fi képes telefonfülkét telepít Manhattan-ben és további 1000-ret ígér az év végéig. Az IEEE ratifikálja a végleges 802.11g szabványt, hamarosan hitelesítik az első ilyen szabványú termékeket. Ekkor már 112 cég 865 terméke kapja meg a hivatalos Wi-Fi hitelesítést 2000 óta. A WPA támogatását kötelezővé teszik a Wi-Fi hitelesítés folyamatában.

2006

Erre az évre fél milliárd (!) 802.11 szabványt támogató, hitelesített eszköz (Access Point, mobiltelefon, asztali PC, DVD lejátszó és felvevő, MP3 lejátszó, notebook, PDA és egyéb termék) eladását becsülték.

4. Összefoglalás

A biztonság a számítógépes társadalom alapvető kérdése, problémája. Nap, mint nap hallunk rosszindulatú vírusokról, hackerekről akik betörnek védett rendszerekbe, hozzáférnek titkos adatbázisokhoz. Egyre több fogalom válik világossá az átlagos felhasználók körében is, nem csak az IT szakemberek védik adataikat, az óvatosság szerencsére egyre jellemzőbb. Azonban még mindig nagyon sok rendszer működik nagyon rosszul kvalifikált, vagy még rosszabb esetben, minden nemű védelmi rendszer alkalmazása nélkül.

Szakdolgozatomban megpróbáltam rávilágítani arra, hogy bár sok előnye van a vezeték nélkül hálózatoknak, a hagyományos vezetékes rendszerekhez képest, ugyanakkor a hátránya, pont ebben a kényes témában, a biztonság témájában mutatkozik meg. Belátjuk, hogy az információ továbbításának eszköze, a levegő egy olyan nyílt közeg, amihez egy rosszindulatú hozzáértő, akár az utcán sétálva, az autójában ülve, vagy velünk egy légtérben tevékenykedve hozzáférhet. A hackerek lehetősége az adatforgalom monitorozására, az értékes erőforrásokhoz történő jogosulatlan hozzáférés, a vezeték nélküli hálózat valamennyi szolgáltatásának megtagadása stb. mind olyan probléma, amelyre nagyon is oda kell figyelni. Ahogy erre több indokot is láttunk, hatékony titkosítás és hitelesítés alkalmazásával a veszély nagymértékben csökkenthető. Azonban tartsuk szem előtt azt a tényt, hogy a biztonság szükséges szintje a követelményektől függ! Egy otthoni alkalmazásnál a biztonság elfogadható szintje lényegesen alacsonyabb, mint amire a vállalatoknál szükség lehet. Ez persze nem azt jelenti, hogy otthon a személyi számítógépünkön lévő információkat nem kéne olyan mértékben védelmeznünk, csak esetleg egy magasabb fokú védelmező eljárás alkalmazása már túlmutathat egy ilyen rendszer keretein.

5. Irodalomjegyzék

[Buttyán] *WiFi biztonság – A jó, a rossz, és a csúf* - Buttyán Levente és Dóra László
Budapesti Műszaki és Gazdaságtudományi Egyetem
Híradástechnikai tanszék
CrySyS Adatbiztonság Laboratórium
[Geier]CISCO SYSTEMS – 2005 Panem Könyvkiadó– Jim Geier Vezeték nélküli hálózatok Wireless Networks First Step.
[Gast]Matthew Gast 802.11 Wireless Networks The Definitive Guide Oreilly Excellent 2002.
[Prasad]Ramjee Prasad, Marina Ruggieri - Artech-Technology Trends in Wireless Communications 2003.
[Khan]Jahanzeb Khan, Anis Khwaja - Building Secure Wireless Networks with 802.11 (Wiley) Wiley publishing inc. 2003.
[Roshan]Pejman Roshan, Jonathan Leary - Cisco.Press,.802.11.Wireless.LAN.Fundamentals.(2003)
[Flickenger]Rob Flickenger - O'Reilly - Building Wireless Community Networks 2002.
[Ouellet]Eric Ouellet, Robert Padjen, Arthur Pfund - Syngress Building A Cisco Wireless Lan 2002.
[Barners]Christian Barners, Tony Bautts, Donald Lloyd - Syngress Hack Proofing Your Wireless Network 2002.
[Barken]Lee Barken - Syngress.-.Wireless.Hacking.Projects.for.Wi-Fi.Enthusiasts[DDU][Share-Books.net] 2004.
[EAP] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz. Extensible Authentication Protocol (EAP). RFC 3748. 2004.
[Edney+04] J. Edney, W. Arbaugh. *Real 802.11 Security: WiFi Protected Access and 802.11i*. Addison-Wesley, 2004.
[Fluhrer+01] S. Fluhrer, I. Mantin, A. Shamir. Weaknesses in the key scheduling algorithm of RC4. Proceedings of the 8th Workshop on Selected Areas in Cryptography. 2001.
[RADIUS] B. Aboba, P. Calhoun. RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP), RFC 3579, 2003.
[Walker00] J. Walker. Unsafe at any key size: An analysis of the WEP encapsulation. *IEEE 802.11-00/362*, 2000.
[WPA] Wi-Fi Alliance. Wi-Fi Protected Access.
[802.11] IEEE Std 802.11. IEEE Standard: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.
[802.11i] IEEE Std 802.11i. IEEE Standard Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.
[PDAMANIA]http://www.pdamania.hu/
[HOWICO]http://www.huwico.hu