DEBRECENI EGYETEM

INFORMATIKAI KAR

Vezeték nélküli hálózatok biztonsági kérdései

Szakdolgozat

Konzulens:

Dr. Krausz Tamás
Egyetemi adjunktus

Készítette:

Tóth Gábor
Programtervező informatikus

Debrecen
2009.

Tartalomjegyzék

Bevezető

A mai világban, a gépek mobillá válásával egyidőben, egyre nagyobb igény van mobil, összekötő vezetéket nélkülöző hálózatokra. Manapság az egyetemeken is egyre több diáknak van laptopja, a géptermek száma pedig véges. Nagy előnyt jelent ilyenkor a vezeték nélküli hálózat, hiszen akár a büféből is intézhetik tanulmányi ügyeiket, megnézhetik órarendjüket, nincsenek időhöz, vagy esetünkben géptermekhez kötve. A vezeték nélküli hálózati technológia tökéletes lehet az olyan munkahelyeken is, ahol sok az úgynevezett mozgó felhasználó. Például az informatikus elsődleges gépe manapság a laptop, amellyel szabadon mozoghat az épületen belül – iroda, tárgyaló, kávézó, udvar – anélkül, hogy megszűnne a hálózati kapcsolata. Persze ezt ki lehet terjeszteni a kedvenc kávézóra, könyvtárra, a parkra, a vonatállomásokra, repülőterekre és az otthoni nappalira, hiszen mindenhol jól jöhet a vezeték nélküli hálózati kapcsolat.

Napjainkban már olcsóbb és gyorsabb a vezeték nélküli hálózat kiépítése, mint a vezetékes. Olyan helyzetekben, amikor a vezetékes hálózat költséges, nem megfelelő, vagy esetleg nem lehetséges a szükséges kábelek lefektetése, a vezeték nélküli hálózati kapcsolatok helyettesíthetnek, vagy akár ki is egészíthetnek egy vezetékes struktúrát. Ha például két épület között szeretnénk kialakítani internetes kapcsolatot, akkor választhatunk egy telekommunikációs szolgáltató által biztosított kapcsolatot állandó telepítési költségért és rendszeres havidíjért, vagy pedig kiépíthetünk egy vezeték nélküli kapcsolatot állandó telepítési díjért, havi üzemeltetési költségek nélkül. A vállalatok számára jelentős, havonta érzékelhető költségmegtakarítást jelent, ami nem egy elhanyagolható dolog a mai gazdasági helyzetben.

Vezeték nélküli hálózati technikával olyan ideiglenes hálózat is létrehozható, amely csupán adott ideig sugároz, üzemel. Például konferencián, rendezvényeken, termékbemutatókon. Ezeket könnyebb kiépíteni, mint a hagyományos Ethernet technológiával létrehozott kábeles hálózatokat. Ha saját házainkat nézzük, ott is praktikusabb és egyszerűbb egy vezeték nélküli hálózat kialakítása a lakás területén, mint a kábelek miatt a falakat furkálni.

A vezeték nélküli hálózatok használata kényelmes, viszont biztonsági problémákat idéz elő, egy sor biztonsági kérdést vet fel. Vezeték nélküli hálózatok esetében az adatcsomagok, a vezetékes technikával ellentétben, nem a kábeleken, hanem a levegőben közlekednek általában rádióhullámok segítségével. Ezeket a hullámokat a falak sem állítják meg, tehát a hagyományos védekezési technikák, bezárt ajtók, biztonsági őrök semmit sem tehetnek a vezeték nélküli hálózaton terjedő adatok védelmében. Vezeték nélküli hálózatok esetében a biztonság nem egy kapcsoló, amit ha bekapcsolunk, akkor van, ha kikapcsoljuk, akkor nincs. A biztonság relatív dolog – csak biztonságosabb, és kevésbé biztonságos rendszer létezik. A biztonság ezen felül dinamikus is – az emberek, technika, folyamatok egyaránt változnak. Ezért is nehéz a biztonságkezelés.

Szakdolgozatomban a vezeték nélküli helyi hálózatoknál felmerülő biztonságtechnikai problémákkal, a lehetséges védelmi módszerekkel szeretnék foglalkozni. A dolgozat elején bemutatom a vezeték nélküli helyi hálózat fejlődésének lépéseit, a hozzá tartozó 802.11 szabványrendszert, annak részeit, alszabványait, magát a vezeték nélküli helyi hálózatot (WLAN). Bemutatom a jelenleg használt hitelesítési, titkosítási, adatintegritási eljárásokat, aztán pedig leírom a támadási módszereket, amelyeknél a támadó a biztonsági hiányosságokat, réseket használja ki. Szakdolgozatom végén pedig tanácsokat adok, hogy egy vezeték nélküli hálózat kialakításánál és konfigurálásánál mire kell és érdemes odafigyelni adataink biztonsága érdekében.

Vezeték nélküli helyi hálózatok (WLAN)

A vezeték nélküli hálózatok kialakulása és fejlődése

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.

1971

Ez a chip inspirált néhány kutatót a Hawaii Egyetemen arra, hogy létrehozzák az első csomag (packet) alapú rádiós adatátviteli technológiát. Ez lett az első vezeték nélküli hálózat (WLAN), s végül is az ALOHAnet nevet kapta. Ez a hálózat 7 számítógépből állt és kétirányú csillag topológia kialakítású volt. Az ALOHAnet négy tagját ölelte fel a Hawaii-szigeteknek, a központi számítógép az Oahu szigeten volt. Ezzel megszülettek a vezeték nélküli hálózatok.

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 (Institute of Electrical and Electronic Engineers) megkezdi a vezeték nélküli kapcsolat szabványának kidolgozását az ISM (Industrial, Scientific and Medical - Ipari, Tudományos és Orvosi) spektrum sávban.

1997

Az IEEE ratifikálja a 802.11 "over-the-air" vezeték nélküli kliensek és alap-állomások közötti interfészt, 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 WiFi 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 anélkül váltani a WiFi és 3G hálózatok között, hogy megszakadna internet kapcsolatuk.
A WECA új szervezetté alakul, WiFi Alliance (WFA, WiFi szövetség) néven, elindítja a 802.11a hitelesítő tesztjeit illetve és bejelenti a WPA (WiFi Protected Access, WiFi védett hozzáférés) biztonsági módszert a WEP leváltására.

2003

A WFA elindítja WiFi 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 WiFi 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 WiFi hitelesítést 2000 óta.
A WPA támogatását kötelezővé teszik a WiFi hitelesítés folyamatában.

2004

2004.június 24.-én elfogadják a 802.11i szabványt, ami fejlődést jelent a vezeték nélküli helyi hálózathasználat biztonságában.

2005

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, amit a tényleges eladás jóval felülmúlt.

Napjainkban már gyakorlatilag minden ember számára elérhetőek a vezeték nélküli eszközök a legújabb biztonsági technikával felvértezve. Egyre több helyen kapcsolódhatunk ingyenes Hotspot- okhoz. Egyre több kávéház, könyvtár, benzinkút, étterem csábítja az embereket WiFi csatlakozási lehetőséggel. Egyre több háztartás szerez be vezeték nélküli adattovábbításra is alkalmas router-t, hogy kényelmesebbé tegye mindennapjait.

IEEE 802.11 szabványok

Már kevéssel a vezetékes számítógépek megjelenése után több csoport is elkezdett módszereket kidolgozni azon cél érdekében, hogy a körülményes vezetékes csatlakozás elhagyásával lehessen valamilyen módon csatlakozni az internetre. A legéletképesebb elgondolás az volt, hogy mind az asztali, mind a noteszgépeket ellátták kis hatósugarú adóvevőkkel, lehetővé téve így köztük a kommunikációt. A probléma ezzel az volt, hogy nagyon sokféle megoldás született, amik inkompatibilisek voltak egymással. Ezért az ipar úgy döntött, hogy jó ötlet lenne megvalósítani egy egységes szabványrendszert, amely lefekteti a vezeték nélküli helyi hálózatok szabványrendszerét.

Az IEEE (Institute of Electrical and Electronic Engineers) 802.11 a megosztott vezeték nélküli helyi hálózatok ipari szabványa, amely meghatározza a vezeték nélküli kommunikáció számára a fizikai réteget és a MAC – alréteget.

802.11 Fizikai alréteg

Kódolási és átviteli sémákat határoz meg a vezeték nélküli kommunikációk számára. A legelterjedtebbek az alábbi megoldások. Mindegyikük megengedi a MAC keretek egyik állomásról a másikra való továbbküldését, a különbség, az ehhez felhasznált műszaki megoldásban és az elérhető sebességben van.

Infravörös átvitel

Közvetlen rálátást nem igénylő átvitelt alkalmaz 0,85 vagy 0,95 mikronos hullámhosszal. Két sebesség lehetséges: 1 Mb/s, vagy 2 Mb/s. 1 Mb/s esetén olyan kódolási sémát használnak, melyben 4 bites csoportokat kódolnak 16 bites kódszavakba, melyekben tizenöt 0 és egyetlen l-es van - ez az úgynevezett Gray kód (Gray code). Erre a kódra az jellemző, hogy egy kisebb szinkronizációs hiba csak egy bithibát okoz a kimeneten. 2 Mb/s esetén a kódolás 2 bitből állít elő 4 bites kódszavakat, melyekben szintén csak egy darab l-es van, vagyis a lehetséges kódszavak a 0001, 0010, 0100 és az 1000. Az infravörös jelek nem képesek áthatolni a falakon, ezért a különböző helyiségekben lévő cellák jól elkülönülnek egymástól. A kis sávszélesség miatt (és amiatt, hogy a napfény elnyomja az infravörös sugarakat) mégsem népszerű ez a változat.

Rádió frekvenciás átvitel

Frekvenciaugrásos szórt spektrumú (FHSS)

Az FHSS (Frequency Hopping Spread Spectrum - frekvenciaugrásos szórt spektrum) a 2,4 GHz-es ISM-sáv aljától kezdődően 79 darab 1 MHz széles csatornát használ. Az ugrások alapját képező frekvenciasorozatokat álvéletlenszám generátor segítségével állítják elő. Ha az állomások ugyanazt a kezdőértéket (seed) használják az álvéletlenszámok előállítására és időben szinkronban maradnak, akkor ugyanazokat a frekvenciákat fogják egyszerre végigjárni. Az egyes frekvenciákon eltöltött, úgynevezett tartózkodási idő (dwell time) állítható paraméter, de értéke nem lehet több 400 ms -nál.

Az FHSS a véletlenszerűség révén ésszerű spektrum felhasználást biztosít a szabályozatlan ISM-sávban. Az eljárás némi biztonságot is ad, hiszen az a betolakodó, aki nem ismeri az ugrási sorozatot vagy a tartózkodási időt, nem tudja lehallgatni az átvitelt. Nagyobb távolságok áthidalásakor gondot okozhat még a többutas csillapítás (multipath fading), de az FHSS ez ellen is jó védelmet biztosít. Az eljárás viszonylag kevéssé érzékeny a rádiós interferenciára, emiatt közkedvelt az épületek közötti kapcsolatok kiépítésénél. Legfőbb hátránya a kis sávszélessége.

Direkt frekvenciaszórásos szórt spektrumú (DSSS)

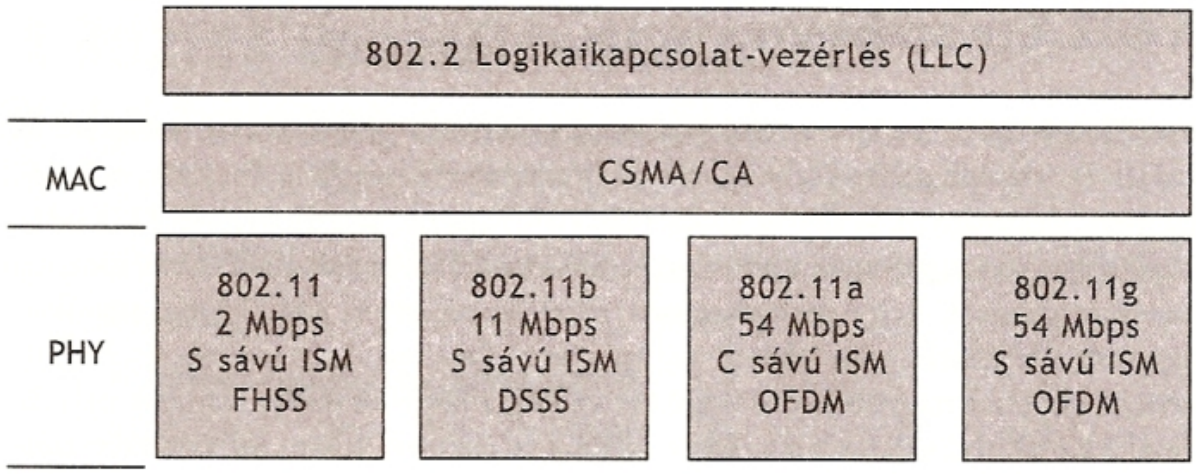
A DSSS (Direct Sequence Spread Spectrum - közvetlen sorozatú szórt spektrum), melynek átviteli kapacitása szintén 1 vagy 2 Mb/s -ra korlátozódik. Minden bitet 11 chip formájában visznek át - ezt a módszert Barker-sorozatnak (Barker sequence) nevezik. A módszer 1 Mbaud -os fázismodulációt használ: baud -onként 1 bitet visz át 1 Mb/s -os működésnél, és 2 bitet a 2 Mb/s -os működésnél. Az FCC éveken át megkövetelte, hogy az Egyesült Államokban az ISM-sávban működő összes vezeték nélküli kommunikációs eszköz szórt spektrumot használjon, de 2002 májusában eltörölték ezt a megszorítást az új megoldások megjelenése miatt.

Ortogonális frekvenciaszórásos multiplexelés (OFDM)

Az első nagysebességű vezeték nélküli LAN, a 802.11a az OFDM (Orthogonal Frequency Division Multiplexing - ortogonális átviteli frekvenciaosztásos multiplexelés) eljárás segítségével akár 54 Mb/s -os átvitelre is képes a szélesebb, 5 GHz -es ISM sávban. Ahogy az FDM rövidítés is jelzi, itt különböző frekvenciákat használnak, mégpedig 52-t, ebből 48-at az adatok számára, 4-et pedig a szinkronizációhoz.

Mivel egyidejűleg több frekvencián is történik átvitel, az eljárás eltér a CDMA-tól és az FHSS-től is, bár szintén a szórt spektrum egy változatának tekinthető. A jel több, keskeny sávra való osztásának fontos előnyei vannak az egyetlen, széles sáv használatával szemben: ilyen például a jobb keskenysávú interferenciatűrés és a nem-folytonos sávok használatának lehetősége.

A bonyolult kódolási rendszer 18 Mb/s -ig fázisbillentyűzésen, onnantól kezdve pedig a QAM -en alapszik. 54 Mb/s-on 216 adatbitet kódolnak 288 bites szimbólumokba. Az OFDM kifejlesztését részben az európai HiperLAN/2 rendszerrel való kompatibilitás motiválta. Ezt az eljárást bit/Hz -ben kifejezve jó spektrumhatékonyság jellemzi, valamint jól ellenáll a többutas csillapításnak is.



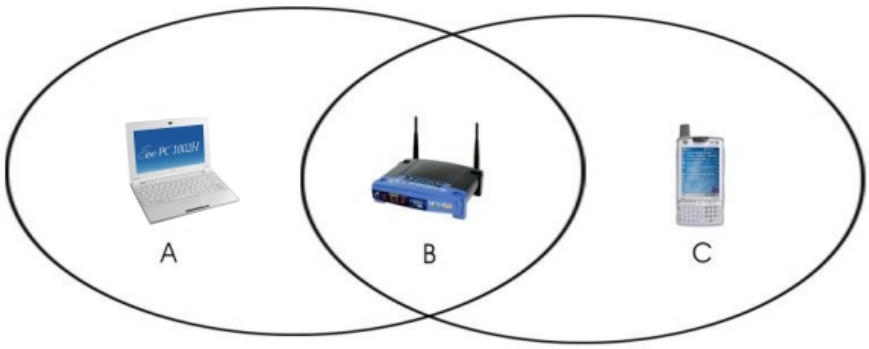
1.ábra: a 802.11 szabványai és a Fizikai réteg

Ezek a rádiófrekvenciás átviteli módok a 2.4 GHz-es ISM sávban működnek, amihez nincs szükség külön engedélyre. A rádióvezérlésű garázsajtó-nyitók is ezt a tartományt használják, úgyhogy elképzelhető, hogy a hordozható számítógépünk egyszer csak a garázsajtónkkal találja majd magát szemben. A zsinór nélküli telefonok és a mikrohullámú sütők szintén ezt a sávot használják. Az összes ilyen berendezés 1 vagy 2 Mb/s -on működik, és elég alacsony a teljesítményük ahhoz, hogy ne zavarják egymást túlságosan.

802.11 MAC alréteg

A MAC alrétegen az összes 802.11 szabvány a többszörös hozzáférésű vivőérintkezést CSMA (Carrier Sense Multiple Access) használja, ütközés elkerüléssel CA (Collision Avoidance) . Egy vezeték nélküli állomás, mielőtt adni kezdene, figyeli a vezeték nélküli frekvenciát, hogy esetleg egy másik állomás éppen küld-e adatokat. Ha érzékel másik állomást, akkor kiszámol egy véletlenszerű visszatartás-késleltetést, majd újra próbálkozik. A CSMA/CA nem képes kiküszöbölni minden ütközést, és egy adó állomás számára nehéz feladat annak érzékelése, hogy ütközés történt.

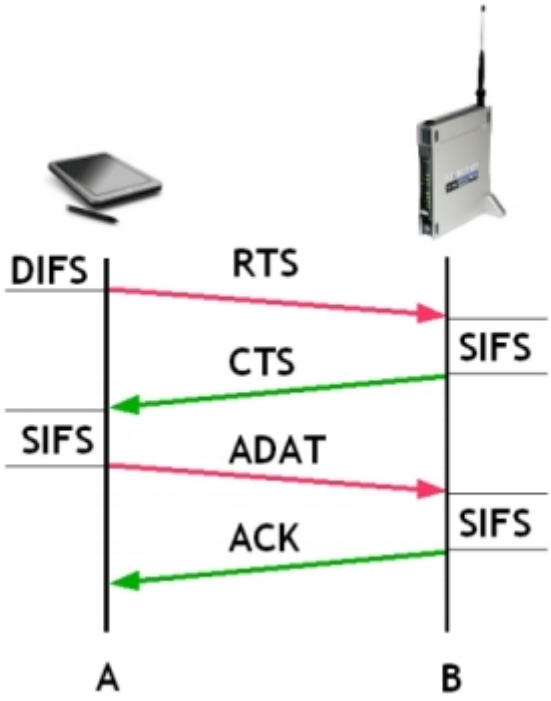
Előfordulhat az is, hogy a hozzáférési pontok AP(esetünkben B) és a vezeték nélküli csomópontok (esetünkben A és C) fizikailag úgy helyezkednek el egymáshoz képest, hogy a csomópontok nem látják egymást, ezért nem érzékelik, hogy a másik csomópont éppen sugároz-e az AP felé. Ezek az úgynevezett rejtett állomások (Hidden Station).



2.ábra: rejtett állomás

Annak érdekében, hogy jobban tudja kezelni az ütközéseket és a rejtett állomásokat bevezetésre kerültek a nyugtázó keretek (ACK), adáskérő (RTS), adásengedélyező (CTS) üzenetek. A nyugtázó keretek jelzik, hogy a vezeték nélküli keretet sikeresen fogadták. A kommunikálni kívánó állomás „A" először egy RTS kerettel jelzi, hogy adni kíván. Erre a másik fél, „B" az általa véletlenszerűen sorsolt idő (SIFS) eltelte után egy CTS üzenetet küld. Amennyiben „A" sikeresen megkapta a CTS keretet, hasonlóan „B"-hez, egy véletlenszerű SIFS idő múlva elkezdi az adást, ha nem kap ilyet, akkor vár egy véletlenszerű ideig (DIFS) és újra küld egy RTS keretet, a procedúra elölről kezdődik, mindaddig, amíg „B" válaszol.

A sikeres adatküldés után „B" egy nyugtázó ACK (Acknowledgement) üzenettel jelzi, hogy megkapta az adatot. Amennyiben az adóállomás nem kap nyugtát, újra kell kezdenie az egész folyamatot. Az RTS és CTS kerekkel kiegészített kommunikációt virtuális vivőérzékeléses mechanizmusnak, más néven „négy utas kézfogás"-nak (Four Way Handshaking) nevezik.



3.ábra: négy utas kézfogás

802.11 szabvány

Az eredeti 802.11 szabvány normál bitsebessége 2, vagy 1 Mb/s, amelyhez az FHSS átviteli sémát és az S sávú, Ipari, Tudományos és Orvosi (ISM) frekvencia sávot használja, amely 2.4 – 2.5 frekvencia tartományba esik.

A 802-es szabványok összes változatának szerkezetében - beleértve az Ethernetet is - van valami közös. A fizikai réteg nagyjából az OSI fizikai rétegének felel meg, az adatkapcsolati réteg viszont minden 802-es protokollban két vagy több alrétegre bomlik.

A 802.11 esetében a MAC (Medium Access Control - közegelérési alréteg) dönt a csatornakiosztásról, vagyis arról, hogy ki lesz a soron következő adó. Fölötte található az LLC (Logical Link Control - logikai kapcsolatvezérlés) alréteg, melynek az a feladata, hogy elrejtse a különböző 802-es változatok eltéréseit, és a hálózati réteg szempontjából megkülönböztethetetlenné tegye őket.

802.11b

A 802.11b működési sebessége a gyakorlatban, ideális esetben 11 Mb/s. A 802.11b lassúbb ugyan a 802.11a-nál, de 7-szer nagyobb működési tartománnyal rendelkezik, ami sok esetben fontos lehet. Az S sávú ISM használatával két további sebességet is használhat (5,5 Mb/s és 11 Mb/s). a magasabb bitsebesség elérése érdekében a DSSS átviteli sémát használja. Sávszélességét tekintve 11Mbit/másodperc 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 másolása 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 hozzáférési pontra (AP) történő tiszta rálátás esetén.

802.11a

Ez volt az első szabvány, amit jóváhagytak, de csak jóval később kezdték el telepíteni széles körben. Akár 54 Mb /s sebességgel is dolgozhat, a C sávú ipari, tudományos és orvosi frekvencia sávot használja, ami 5.725 és 5.875 GHz közötti frekvenciatartományt jelent. A szabvány DSSS helyett OFDM-et használ, amely lehetővé teszi, hogy párhuzamosan, alfrekvenciákon is továbbítson adatokat. Nagyobb az átviteli képessége és nagyobb ellenállással rendelkezik az interferencia ellen is.

Ez a nagyobb sebességű technológia lehetővé teszi a vezeték nélküli hálózathasználatot arra, hogy jobban teljesítsen video, és konferencia alkalmazásokban. Mivel nem ugyanazon az S sávú frekvencián dolgoznak, mint a többi eszközök, ezért magasabb átviteli sebességet és tisztább jelet szolgáltat. 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

Az IEEE-nek sok fejtörést okozott, hogy melyik szabadalmaztatott megoldást használja, míg végül 2001 novemberében elfogadta a 802.11b továbbfejlesztett változatát, a 802.11g-t. Ez is az S ISM sávot használja, OFDM-vel. Visszafelé kompatibilis a 802.11b szabvánnyal, képes dolgozni a 802.11b szabvány bitsebességével és DSSS-t használni. A 802.11g hálózati adapterek képesek csatlakozni a 802.11b vezeték nélküli hozzáférési pontokhoz. 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/s -ot jelent a valóságban. Hatótávolsága épületen belül 30-50 méter.

Az IEEE 802.11x szabványcsalád			
Alszabvány neve	*Frekvenciasáv*	*Maximális adatátviteli sebesség*	*Modulációs technikák*
802.11	2,4 Ghz	1 vagy 2Mbps	DBPSK, DQPSK
802.11a	5,7 Ghz	6-54 Mbps	OFDM
802.11b	2,4 Ghz	2-11 Mbps	DSSS, CCK
802.11g	2,4 Ghz	2-54 Mbps	DSSS, CCK, OFDM, DSSS-OFDM
802.11i	-	-	Biztonságtechnikai alszabvány.

4.ábra : az IEEE 802.11 szabványcsalád

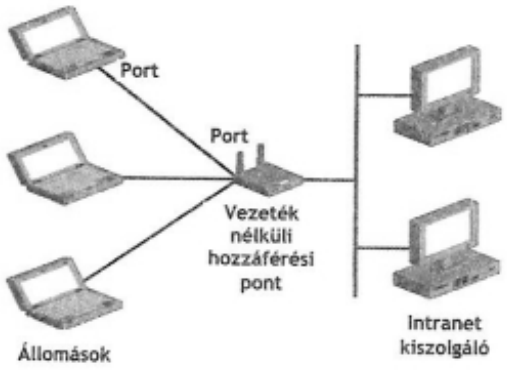
A 802.11-en alapuló vezeték nélküli LAN-ok telepítése szerte a világon folyamatosan bővül, az irodaépületekben, repülőtereken, hotelekben, éttermekben és egyetemeken. Ez a terület várhatóan gyors fejlődésen fog átmenni. De melyiket válasszam?

Ma már a legtöbb termék olyan, amely mindhárom szabványt ismerik. Ha vásárlásra kerül a sor, érdemes ezt figyelembe vennünk, bár természetesen némileg drágábbak a sima b/g képes eszközöknél. A G változatok egyéb iránt alig kerülnek valamivel többe, mint a B –s termékek, ez a kis plusz kiadás tehát nagyon is megéri az árát.

A vezeték nélküli helyi hálózatok összetevői

Az IEEE 802.11 vezeték nélküli helyi hálózathasználat a következő elemekből épül fel:

- Állomások
- Vezeték nélküli hozzáférési pontok
- Portok



5.ábra: A 802.11 vezeték nélküli helyi hálózathasználat

Állomások

Az állomás (STA, station) tulajdonképp egy olyan számítási kapacitással rendelkező berendezés, melyet vezeték nélküli helyi hálózati csatolóval rendelkezik. Például az olyan személyi számítógépet, amelyet vezeték nélküli csatolóval szereltek fel, vezeték nélküli ügyfélként is tekinthetjük. Ezen ügyfelek képesek egymással közvetlenül, vagy vezeték nélküli hozzáférési ponton keresztül kommunikálni. Egy állomás lehet mozdulatlan, vagy mobil.

Vezeték nélküli hozzáférési pontok

Az olyan hálózati eszközt nevezzük vezeték nélküli hozzáférési pontnak, amely rendelkezik egy vezeték nélküli helyi hálózati csatolóval. Tulajdonképp felfoghatjuk egy hídnak, amely összeköti a hagyományos vezetékes hálózatokat, a vezeték nélküli állomásokkal. Egy hozzáférési pontnak biztosan tartalmaznia kell a következő összetevőket:

- Interface, amely a hozzáférési pontot összeköti a hagyományos vezetékes hálózattal
- Egy rádiójelet sugárzó berendezés, amely tartja a kapcsolatot a vezeték nélküli ügyfelekkel (állomásokkal).
- Hídszoftver, amely arra hivatott, hogy az eszköz átviteli hídként szolgáljon a vezeték nélküli és a vezetékes hálózatok között.

Portok

Az eszközök olyan logikai csatornáit nevezzük portoknak, amelyek pont-pont típusú kapcsolatot tesznek lehetővé. A 802.11 esetén egy port egy kapcsolatot jelent. Egy olyan logikai egységet, melyen keresztül magában álló vezeték nélküli kapcsolat jön létre. Egy vezeték nélküli ügyfél több porttal is rendelkezik, és több vezeték nélküli kapcsolatot is képes használni. A logikai kapcsolat egy vezeték nélküli hozzáférési pont és egy vezeték nélküli ügyfélhez tartozó port között, pont-pont hidalt helyi hálózati szegmenst alkot. Minden egyes keret, melyet egy vezeték nélküli ügyféltől küldtek, az ügyfél, és a hozzáférési pont közötti pont-pont LAN szegmensre megy.

Az IEEE 802.11 üzemmódjai

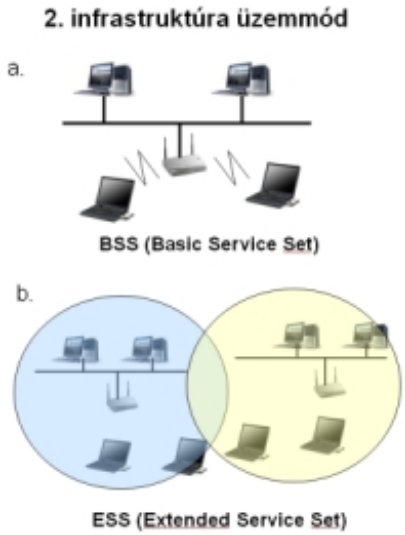
Az IEEE szabvány a következő működési módokat határozza meg:

- Infrastruktúra üzemmód
- Eseti (ad-hoc) üzemmód

Ezen üzemmódoktól függetlenül van egy úgynevezett szolgáltatáskészlet azonosító, SSID (Service Set Identifier), melyet a vezeték nélküli hálózat neveként is emlegetnek, hiszen azonosítja a vezeték nélküli hálózatot. Az SSID-t a hozzáférési pont időnként meghirdeti, egy úgynevezett jelzőkeretet (beacon frame) használva.

Infrastruktúra üzemmód

Infrastruktúra üzemmódban a hálózatot legalább egy vezeték nélküli hozzáférési pont és egy vezeték nélküli ügyfél alkotja. A vezeték nélküli ügyfél a hozzáférési pontot használja arra, hogy kapcsolatot teremtsen egy hagyományos vezetékes hálózati szolgáltatással. Ez a hagyományos hálózat, a vezeték nélküli hálózati pont elhelyezkedésétől függően lehet akár egy cég helyi hálózata, vagy maga a világháló is.



6.ábra: infrastruktúra üzemmód

Ha egy vezeték nélküli hozzáférési pont van, amely több vezeték nélküli ügyfél kiszolgálására képes, akkor alap szervizkészletről (BSS, Basic Service Set) beszélünk. Ha több vezeték nélküli hozzáférési pont, ugyanazon vezetékes hálózathoz kapcsolódva egy logikai szegmenst határoz meg, amelyet egy útválasztó köt össze, akkor kibővített szervízkészletről (ESS, Extended Service Set) beszélünk.

Ha egy vezeték nélküli hálózati csatolót bekapcsolnak, az elkezd pásztázni (scanning), keresni vezeték nélküli hálózati pontok, és más vezeték nélküli ügyfelek frekvenciái után. A csatolók próbakérő-kereteket küldenek az ISM frekvenciatartomány minden csatornáján, és figyelik a vezeték nélküli pontok és más vezeték nélküli ügyfelek próbaválasz-kereteit. Ezen pásztázási folyamat után a vezeték nélküli csatoló választ magának egy hozzáférési pontot, amelyhez csatlakozhat. Ezek után a vezeték nélküli ügyfél egyeztet a port használatáról a hozzáférési ponttal. Ez a folyamat az úgynevezett társítás (association).

Ha a vezeték nélküli hozzáférési pont jelerőssége túl alacsony, ha a hibaarány túl magas, akkor a vezeték nélküli ügyfél új, erősebb jelet biztosító hozzáférési pont után kutat. Ha talál ilyet, akkor egyeztet a hozzáférési ponttal. Ez a folyamat újra-összerendelésként (reassociation) ismert. Több okból is kerülhet sor újra-összerendelésre:

- A jel legyengülhet
- A vezeték nélküli ügyfél távolabb kerül a hozzáférési ponttól
- A hozzáférési pont túlnépesedik a túl sok egyéb forgalom miatt

Eseti (ad-hoc) üzemmód

Eseti (ad-hoc) üzemmódban a vezeték nélküli ügyfelek közvetlenül, vezeték nélküli hozzáférési pont használata nélkül kommunikálnak egymással. Az eseti üzemmódot, egyenrangú (peer-to-peer) üzemmódnak is nevezik. A vezeték nélküli ügyfelek eseti üzemmódban, úgynevezett független alap szervizkészletet (IBSS, Independent Basic Service Set) képeznek. A vezeték nélküli ügyfelek egyike, az IBSS -ben lévő első vezeték nélküli ügyfél lesz, amely valamennyit átvesz a vezeték nélküli pont kötelezettségeiből.

Ilyen kötelezettségek például a periodikus jelzőfolyamat és az új ügyfelek hitelesítése. Akkor használjuk az ad-hoc üzemmódot, ha nincs jelen vezeték nélküli kapcsolódási pont. A 802.11 szabványnak megfelelő eseti üzemmódban működtetett vezeték nélküli hálózatban legfeljebb kilenc tag lehet. Ez a módszer - nevéből adódóan - alkalomszerű, azaz olyan esetben érdemes használni, amikor gyorsan, rövid időre kell összekapcsolnunk két eszközt, vagy ez a legolcsóbb módja a kommunikációnak (vezetékes kapcsolattól eltekintve), például át szeretnénk másolni néhány fájlt, vagy kedvenc játékunk többjátékos üzemmódjában szeretnénk játszani ismerősünkkel.

7.ábra: ad-hoc üzemmód

Vezeték nélküli adatvédelem

A vezeték nélküli hálózatok, a vezetékes (Ethernet) hálózathasználati technikától eltérően, rádiójelek segítségével sugározzák szét az adatokat, ezért az átviteli közeghez való hozzáférést nehéz ellenőrizni. Ethernet esetében fizikai hozzáféréshez is szükségünk van, hogy csatlakozni tudjunk, vezeték nélküli technika esetén, még arra sincs szükség, hogy az épületen belülre kerüljünk, hiszen a rádiójeleket nem állítják meg a falak, így akár az utcáról is hozzáférhetünk a hálózathoz. Vezetékes hálózatoknál az adatforgalom titkosításáról sem kell gondoskodnunk, hiszen a zárt hozzáférés miatt az adatok, az engedély nélküli felhasználók számára nem elérhető kábelezési rendszeren át folynak. Vezeték nélküli hálózatok esetén viszont szükséges a titkosítás, hiszen a hálózatra bárki rácsatlakozhat, aki

rendelkezik a szükséges vezeték nélküli eszközökkel, és az összerendelési tartományon belül van. Ezért a vezeték nélküli helyi hálózatok számára az adatvédelem, annak megvalósítása és bevezetése a technológia nélkülözhetetlen elemének számít.

A vezeték nélküli hálózatok biztonságos kommunikációja a következőkkel kell, hogy rendelkezzen:

- Hitelesítés
- Titkosítás
- Adatintegritás

Hitelesítés:

Mielőtt elkezdődne az adatforgalom cseréje a vezeték nélküli hálózattal, a csomópontnak azonosítania kell magát, és a hitelesítési módszertől függően, hitelesítési adatokat kell küldenie, amelyek validálhatóak.

Titkosítás:

Egy adatcsomag elküldése előtt, a vezeték nélküli csomópontnak gondoskodnia kell az adatok bizalmasságáról, ezért titkosítania kell azokat.

Adatintegritás:

A vezeték nélküli csomópontnak az adatcsomag elküldése előtt be kell építenie a csomagba olyan információt is, amelynek segítségével a címzett ellenőrizni tudja, hogy az adatátvitel során nem módosították-e a csomag tartalmát.

Az eredeti IEEE 802.11 szabvány meghatározta a hitelesítést, titkosítást és adatintegritást a vezeték nélküli adatforgalom számára. Mint később látni fogjuk, ez elég sebezhetőnek bizonyult a gyakorlati megvalósításnál.

Hitelesítés

AZ IEEE 802.11 szabvány a következő hitelesítési típusokat határozza meg:

- Nyíltrendszer hitelesítés
- Megosztott kulcsú hitelesítés

Nyíltrendszer hitelesítés:

Nevével ellentétben nem hitelesítést szolgáltat, csak azonosítást a vezeték nélküli adapter közeghozzáférés vezérlés (Media Access Control) MAC címét felhasználva. Ezt akkor használják, ha nincs szükség hitelesítésre.

Ebben az esetben az alapértelmezett hitelesítési algoritmus a következő:

- A vezeték nélküli ügyfél, amelyik a hitelesítést indítani szeretné, elküld egy nyíltrendszer hitelesítést kérő üzenetet, amely tartalmazza a MAC címet, mint a 802.11 keret forráscímét.
- A kérést fogadó vezeték nélküli csomópont nyíltrendszer hitelesítési üzenettel válaszol, amelyben jelzi, hogy sikeres (a kezdeményező ügyfél hitelesítést nyert), vagy sikertelen volt a hitelesítés.

Egyes vezeték nélküli hozzáférési pontok lehetővé teszik, hogy megadjuk számukra előre az összes hitelesített vezeték nélküli ügyfelek MAC címeinek listáját, azonban ez nem biztosít védelmet, hiszen a támadók megszerezhetik a vezeték nélküli csomagokat, és egy érvényes MAC cím klónozásával máris használhatják a hálózatot.

Megosztott kulcsú hitelesítés:

A megosztott kulcsú hitelesítés azt ellenőrzi, hogy a hitelesítést kezdeményező állomás rendelkezik-e egy előre megosztott titok ismeretével. A 802.11 szabvány feltételezi, hogy a kulcs egy biztonságos csatornán eljutott a vezeték nélküli ügyfelekhez. Ennek mikéntjét a

szabvány nem definiálja. Ez a gyakorlatban egy karaktersorozatot jelent, amit a vezeték nélküli hozzáférési pont és a vezeték nélküli ügyfél konfigurálásakor írtak be. A megosztott kulcsú hitelesítés algoritmusa a következő:

- A vezeték nélküli ügyfél, amelyik a hitelesítést indítani szeretné, elküld egy megosztott kulcsú hitelesítést kérő üzenetet
- A hitelesítést érvényre juttató vezeték nélküli csomópont megosztott kulcsú hitelesítési üzenettel válaszol, amely tartalmaz egy kihívó (challenge) szöveget.
- A hitelesítést kezdeményező csomópont válaszol egy megosztott kulcsú hitelesítési kéréskerettel, amely a kihívó szöveg titkosított formáját tartalmazza. A titkosítás a megosztott kulcs felhasználásával történik. Ez a titkosítás a WEP (Wired Equivalent Privacy).
- A hitelesítést érvényre juttató vezeték nélküli csomópont visszakódolja a kapott üzenetet, és ha az eredeti kihívó üzenetet kapta meg a visszakódolás után, akkor sikeres volt a hitelesítés.

Titkosítás és adatintegritás

Az IEEE 802.11 szabványban definiált vezetékessel egyenértékű titkosítás azt célozta, hogy egy olyan szintű adatbizalmasságot és integritást nyújtson, amely egyenértékű a vezetékes hálózatéval. De a vezeték nélküli helyi hálózatok üzenetszóró természete miatt nagyon könnyű az üzeneteinek lehallgatása és távoli figyelése.

WEP (Wired Equivalent Privacy)

Vezetékessel egyenértékű titkosságra utal, amely a vezeték nélküli csomópontok között küldött adatok titkosításával nyújt adatbizalmassági szolgáltatásokat. Hogy az üzenet WEP titkosítással lett elküldve, a 802.11 keretek MAC fejrészében beállított WEP jelző bekapcsolása jelzi. Az adatintegritást az biztosítja, hogy egy integritás ellenőrző értéket (ICV, Integrity Check Value) is tartalmaz a vezeték nélküli keret titkosított részében.

A WEP két megosztott kulcsot is definiál:

- Többes üzenet / globális kulcs
- Címzett kommunikációs munkamenet kulcs

Többes üzenet / globális kulcs

Olyan titkosító kulcs, amely a vezeték nélküli hozzáférési pontról, az összes hozzá kapcsolódó vezeték nélküli ügyfélhez irányuló többes üzenet és üzenetszórási forgalmat védi.

Címzett kommunikációs munkamenet kulcs

Olyan titkosító kulcs, amely védi a címzett üzenetforgalmat egy vezeték nélküli ügyfél és egy vezeték nélküli hozzáférési pont között. Védi a vezeték nélküli ügyfél által a hozzáférési pont felé küldött többes üzenet és üzenetszórási forgalmat.

Az RC4-es algoritmus két részből áll. Van egy kulcs ütemező algoritmusa, és egy csomag generátora. A WEP esetében a kulcs ütemező vagy 64 bites kulcsot használ (40 bites titkos kulcs és a 24 bites IV), vagy 128 biteset (104 bites titkos kulcs, és 24 bit IV), amivel az RC4 állapottömbjét készíti el.

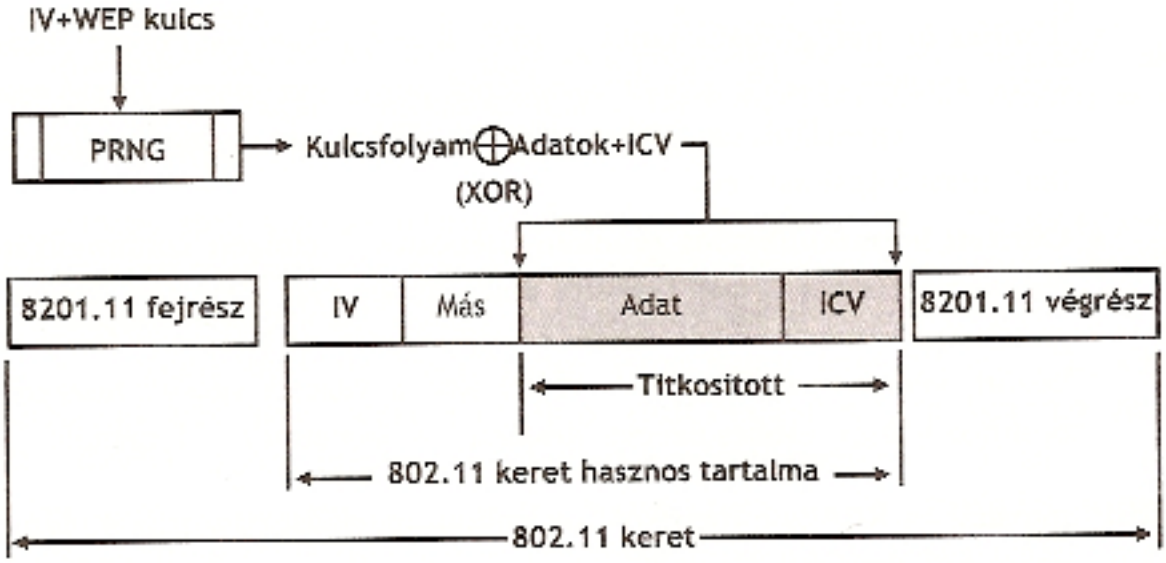
A WEP titkosítás folyamata

Egy 802.11 üzenetkeret titkosítására a következő folyamat szolgál:

- A rendszer a keretadatokból kiszámol egy 32 bites integritás ellenőrzési összeget.
- A kiszámolt ellenőrző összeget a keretadatok végéhez fűzi hozzá.
- Egy 24 bites IV képződik, amit hozzácsatolnak a WEP titkosító kulcshoz.
- A WEP titkosító kulcs és az IV kombinációját egy PRNG (Pseudo-Random Number Generator) bemeneteként használjuk, amely egy olyan bitsorozatot hoz létre, melynek mérete ugyanakkora, mint az adatok és az integritás ellenőrző összegéé.
- A PRNG bitsorozatot, más néven a kulcsfolyamot, a rendszer a hasznos adatok titkosítására használja fel oly módon, hogy a bitenkénti kizáró vagy (XOR) művelettel

hozzákeveri az [adat+ICV] folyamhoz. Ez a titkosított folyam megy át a hozzáférési pont és az ügyfél között.

- Úgy jön létre maga a MAC keret, hogy az IV-t más mezőkkel együtt hozzáadják a titkosított [adatok+ICV] együttes elejéhez.

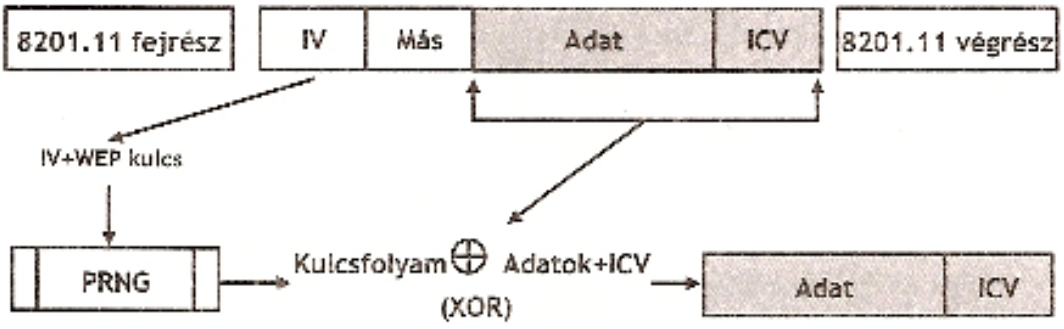


8.ábra: a WEP titkosítási folyamat

A WEP visszafejtés folyamata:

A keretadatok visszafejtéséhez a következő folyamatot használjuk:

- A 802.11 keret hasznos tartalmából kinyerjük az IV-t.
- A WEP titkosító kulcshoz fűzzük az IV-t.
- Az IV és a WEP titkosító kulcs együttesét a PRNG bemeneteként felhasználjuk arra, hogy létrehozzon egy ugyanakkora méretű bitsorozatot, mint az adatok és az IV kombinációja. Ekkor létrehozza ugyanazt a kulcsfolyamot, mint a vezeték nélküli csomópont küldése.
- Ezen adatok logikai összeadásával visszakódolja a hasznos forgalom adat- ICV részét.
- Az eredményt a szoftver összeveti a bejövő keretben található értékkel. Ha ezek az értékek megegyeznek, akkor az adat érvényesnek minősül, vagyis nem módosult a küldés során. Ha nem egyezik meg, akkor a rendszer eldobja a keretet.



9.ábra: a WEP visszafejtési folyamat

Habár a titkos kulcs hosszú ideig állandó marad, az IV keretről keretre változik. Ennek időszakossága a WEP algoritmushoz szükséges titoktartás fokától függ. A WEP hatékonyságának fenntartására az ideális módszer az lenne, ha minden egyes keret után megváltoztatnák az IV-t.

Az IEEE 802.11 szabvány adatvédelmi problémái

A legnagyobb probléma a WEP -pel, hogy a titkosító kulcsok terjesztése és meghatározása nincs értelmezve. A WEP kulcsokat a 802.11 protokollon kívül, biztonságos csatornák használatával kell szétosztani. A gyakorlatban ez úgy néz ki, hogy a kulcsokat, amelyek szöveges karaktersorozatok manuálisan kell bekonfigurálni a billentyűzeten keresztül mind a vezeték nélküli hozzáférési pont, mind a vezeték nélküli ügyfél esetében. Nyilvánvalóan ezt egy nagyvállalati környezet esetén már nem olyan egyszerű koordinálni, és nem is biztonságos.

Nincs meghatározva a WEP titkosító kulcsok változtatásának mechanizmusa sem hitelesítéssel, sem hitelesített kapcsolaton keresztül. Minden ügyfél és csatlakozási pont ugyanazt a manuálisan beállított WEP kulcsot használja több munkameneten keresztül. Főként olyan esetekben, amikor nagyszámú vezeték nélküli ügyfék, nagymennyiségű adatot

küld, akkor a támadó nagymennyiségű WEP rejtjelet tud lehallgatni és jelszóelemzési módszerekkel meg tudja könnyen határozni a WEP kulcsot.

A következő adatvédelmi kérdések merülnek fel az eredeti 802.11 szabvánnyal kapcsolatban:

- Nincs felhasználó szintű hitelesítés és azonosítás
- Hamis vezeték nélküli hozzáférési pontok
- Nincs kialakított mechanizmusa a központi hitelesítésnek, engedélyezésnek, ügyfélkezelésnek
- Egyes implementációk jelszavakból származtatják le a WEP kulcsokat, ami nagyon gyenge WEP-kulcsokat eredményez.
- Nincs támogatás a kibővített hitelesítési módszerekhez sem. Például intelligens kártyákhoz, tanúsítványokhoz, biometrikához, egyszer használatos jelszavakhoz, stb…
- Nincs támogatás a kulcskezeléshez. Például, hogy munkaállomásonként, vagy munkamenetenként dinamikusan újrakódolják a globális kulcsokat.

Az IEEE 802.11 szabvány ilyen gyengeségeinek kiküszöbölésére hozták létre a 802.1x szabványt.

Hitelesítés a 802.1x szabvánnyal

Az IEEE 802.1x szabvány, port alapú hálózati hozzáférés-ellenőrzést használ ahhoz, hogy hitelesített hálózati hozzáférést biztosítson vezetékes Ethernet hálózatokhoz. Az összekapcsolt helyi hálózati infrastruktúra fizikai jellemzőit használja fel, hogy hitelesíthesse a helyi hálózati portokhoz csatlakozó eszközöket. Ha a hitelesítési folyamat sikertelenül zárul, akkor a porthoz való hozzáférés megtagadható. Ezt a szabványt eredetileg vezetékes hálózatok számára tervezték, de adaptálták vezeték nélküli hálózatokhoz is.

A 802.1x szabvány elemei

A szabvány meghatározza a következő szakkifejezéseket is:

- Porthozzáférési egység (PAE, Port Access Entity)

Olyan logikai egység, amely támogatja a porthoz tartozó IEEE 802.1x protokollt. Egy PAE felveheti a hitelesítő, a kérvényező, vagy akár mindkettő szerepét.

- Hitelesítő

Olyan helyi hálózati csatlakozó, amely megköveteli a hitelesítést, mielőtt engedélyezné a hozzáférést a porton keresztül elérhető szolgáltatásokhoz. Egy logikai helyi hálózati port a vezeték nélküli hozzáférési ponton, amelyen keresztül az ügyfelek hozzáférést szerezhetnek más vezeték nélküli ügyfelekhez és vezetékes hálózatokhoz.

- Kérvényező

Olyan helyi hálózati port egy vezeték nélküli hálózati csatlakozón, amely egy hitelesítőhöz kapcsolódva, majd hitelesítve magát hozzáférést kér más vezeték nélküli ügyfelekhez és vezetékes hálózatokhoz.

- Hitelesítő kiszolgáló

A hitelesítő, egy hitelesítő-kiszolgálót vesz igénybe ahhoz, hogy azonosíthassa a kérelmező hitelesítési adatait. Ez a kiszolgáló a hitelesítő nevében ellenőrzi a kérelmező adatait, majd visszajelez a hitelesítőnek, hogy a kérelmezőnek van-e joga a szolgáltatások igénybevételéhez.

A hitelesítő kiszolgáló a következő lehet:

  - A hozzáférési pont egy eleme

    Ebben az esetben a hozzáférési pontot felhasználói hitelesítő adatokkal kell bekonfigurálni, melyek megfelelnek annak a kérelmezőnek, amely megpróbál majd kapcsolódni. Jellemzően nem épül be a vezeték nélküli hozzáférési pontokba.

  - Egy önálló egység

    Ebben az esetben a hozzáférési pont egy külön hitelesítő kiszolgálóhoz küldi a kapcsolódási kísérlet hitelesítési adatait. Jellemzően a vezeték nélküli hozzáférési pont RADIUS-t (Remove Authentication Dial-in User Service, távoli

hitelesítésszolgáltatás betárcsázó felhasználóknak) használ, hogy egy kapcsolatkérési üzenetet küldjön egy RADIUS kiszolgálóhoz.

Szabványos hitelesítési mechanizmusként az IEEE 802.1x szabványhoz az EAP (Extensible Authentication Protocol) kiterjeszthető hitelesítési protokollt választották. Ez egy pont-pont protokoll (PPP) alapú hitelesítési mechanizmus, amelyet a pont-pont hálózati szegmenseken való használathoz adaptáltak.

IEEE 802.11i szabvány

Az IEEE által kidolgozott és jóváhagyott szabvány lényegében egy protokoll (ajánlás) csomag, a meglévő és a jövőbeni fizikai vezeték nélküli hálózatok biztonságának fokozására. A fő hangsúly a hálózati hitelesítésen és annak biztonságosságán van. Lényegében nem teljesen új átviteli protokollokat szabványosít a 802.11i, hanem meglévő, vezetékes környezetben korábban már széleskörűen alkalmazott eljárásokat implementál vezeték nélküli környezetbe.

Tartalma igen szerteágazó, a vezeték nélküli hálózatokban eddig nem alkalmazott hitelesítési metódusokat és kriptográfiai újdonságok sorát vonultatja fel:

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

<u>Új kriptográfiai eljárások:</u>

- CCMP (AES - CCM), TKIP
- Dinamikus kulcs csere és management

WPA

Az IEEE 802.1x szabvány az eredeti 802.11 szabvány sok biztonsági hiányosságát pótolta, még mindig jelentkeztek problémák, amelyek a WEP titkosítás gyengeségeit és adatintegrációs módszereit illeti. Ezen problémák orvoslására elkezdték fejleszteni a 802.11i szabványt, de a vezeték nélküli rendszerek fejlesztői egyetértettek abban, hogy amíg véglegesítik a 802.11i szabványt, addig is elfogadnak egy együttműködésre alkalmas köztes szabványt, ismertebb nevén a Védett vezeték nélküli hozzáférést (WPA, Wi-Fi Protected Access).
Melynek célkitűzései a következők voltak:

- Biztonságos vezeték nélküli hálózathasználat.
  Szükség van hozzá a 802.1x szabvány hitelesítésére, titkosításra és címzett üzenetes és globális titkosítási-kulcs kezelésre.
- A problémák megoldása WEP –pel és szoftverfrissítésekkel.
  A WEP –en belül, az RC4-folyam titkosítás sérülékeny az ismert nyílt szövegű támadásokkal szemben. Továbbá gyenge a WEP által biztosított adatintegritás is. A WPA megoldást nyújt az összes WEP–nél megmaradt biztonsági problémára, csupán a szoftver frissítését igényli, mind a vezeték nélküli eszközök, mind a vezeték nélküli ügyfelek esetében.
- Biztonságos vezeték nélküli hálózathasználati megoldás a kisirodai és otthoni (SOHO) vezeték nélküli felhasználóknak.
  A SOHO felhasználók számára nem áll rendelkezésre RADIUS kiszolgáló, hogy EAP típusú 802.1x hitelesítést adjon. Ezért számukra egyrészt megosztott kulcsos hitelesítést kell használniuk (ami nem javasolt), vagy nyílt rendszerű hitelesítést (ez inkább javasolt), egy egyszerű statikus WEP kulccsal, mind a címzett üzenet, mind a többes üzenetek forgalmához.
- Megoldásként a WPA egy előre megosztott kulcsú opciót kínál. Ezt a kulcsot a vezeték nélküli ponton és az érintett vezeték nélküli ügyfeleken konfigurálják. A hitelesítési folyamatból származik a kezdeti címzett üzenettitkosított kulcsa, amely igazolja, hogy mind a hozzáférési pont, mind az ügyfél rendelkezik az előre megosztott kulccsal.

A WPA adatvédelem szolgáltatásai

Hitelesítés:

Amíg az IEEE 802.11 esetén a 802.1x hitelesítés opcionális, addig WPA esetén kötelező. A WPA hitelesítés a nyílt rendszerű és a 802.1x hitelesítés kombinációja, amely a következő fázisokat használja:

- Első fázisban a nyílt rendszerű hitelesítést használja, ezzel jelezve a vezeték nélküli ügyfélnek, hogy a vezeték nélküli hozzáférési ponthoz keresztüzeneteket küldhet.
- Második fázisban a 802.1x –et használja, hogy egy felhasználói szintű hitelesítést valósítson meg.

RADIUS infrastruktúra nélküli környezetben a WPA támogatja az előre megosztott kulcsok használatát. Valójában ez a megoldás nem hordoz magában 802.1x alapú (EAP) hitelesítési képességeket, tehát nincs EAP (EAPoL) és RADIUS protokoll alapú kommunikáció a két eszköz között.

A WPA-PSK mód általában mindegyik ma megvásárolható eszközön kiválasztható, vagy a régebbi WLAN eszközökhöz új firmware frissítéssel használhatóvá válik. Beállítása egyenként, minden eszközön külön-külön megadott jelszó vagy hexadecimális karaktersorozat (amely a PSK) segítségével történik. A PSK fogja reprezentálni ebben az esetben a RADIUS szervertől kapott PMK kulcsot.

A felhasználói adatok titkosításához használt TK meghatározása „4 utas kézfogással” és véletlenszerűen generált (nonce) számok segítségével történik, azzal a különbséggel, hogy nem EAPoL üzenetekkel, hanem normál üzenetcsomagokkal (1500 bit) történik a kommunikáció.

A PSK és az ebből generált kulcsok itt sem kerülnek átvitelre, a TK meghatározása után AES (CCMP, WRAP) vagy TKIP titkosító algoritmust használhatnak a felhasználói adatok titkosítására. A WPA-PSK módszer használható Ad-Hoc hálózatokban is hitelesítés és

adattitkosítás céljára (mivel Ad Hoc esetben nincs hitelesítést végző és a kommunikációt irányító kitüntetett fél).

RADIUS struktúrával ellátott környezetben pedig az EAP és RADIUS használatát támogatja a WPA.

EAP:

Az EAP nem egy hitelesítési protokoll, inkább egy, korábban a vezetékes hálózatokban már sikerrel alkalmazott adatátviteli technológia. A port megnyitása előtt EAP protokoll segítségével történik a kommunikáció. A WLAN hálózatban a kliens (Mobil Állomás) és a hitelesítési szerver EAP protokoll segítségével kommunikál. Az Access Point ebben a fázisban nem jut szerephez, tehát átlátszó proxy-ként kell viselkednie, át kell engednie a forgalmat a szerver felé és a szervertől a kliens irányába. Az EAP független a hálózat más elemeitől, egyszerre többféle változata is tetszőlegesen használható hitelesítési célokra.

EAP-MD5:

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

LEAP (Lightweight EAP):

Ezt az eljárást a Cisco cég dolgozta ki és használja eszközeiben. Hasonlóan az előzőhöz, MD5 lenyomatokat használ, viszont kétirányú azonosítást kíván meg (szerver és kliens oldalon egyaránt hitelesíteni kell egymást). WLAN eszközökben alkalmazott változata WEP kulcsok cseréjét is támogatja. Homogén, Cisco gyártmányú eszközökkel felépített hálózatban egyszerű lehet a használata, máshol viszont nem ajánlott a kompatibilitási problémák elkerülése végett.

EAP-TLS (Transport Layer Security):

Kétirányú, szerver – kliens azonosítást használ, PKI kulcsinfrastruktúrán alapszik. A TLS az SSL-en (Secure Socket Layer) alapul, melyet elterjedten használnak a WEB-en titkosítás és hitelesítés céljából. A legtöbb kliens platformon (Linux, Windows, MacOS X) telepíthető kliens szoftver vagy modul.

Több szoftverfejlesztő cég RADIUS szerverével (HP, Microsoft, FreeRADIUS.org, stb.) használható. Hátránya, hogy teljes nyílt kulcsú infrastruktúrát igényel (PKI – Public Key Infrastructure), melynek kidolgozása, a tanúsítványok, SMART-Card eszközök (a tanúsítványok egyénhez rendelése és tárolására) beszerzése meglehetősen költséges. Ezzel szemben ez a módszer nyújtja a legnagyobb biztonságot hitelesítés tekintetében.

EAP-TTLS (Tunneled Transport Layer Security):

Annyival egyszerűbb az EAP-TLS -nél, hogy nincs szükség kliens oldali PKI infrastruktúrára, a kliens jelszóval azonosítja magát, tehát lecsökkenthetők a költségek. A szerver oldalon viszont továbbra is szükségesek a tanúsítványok.

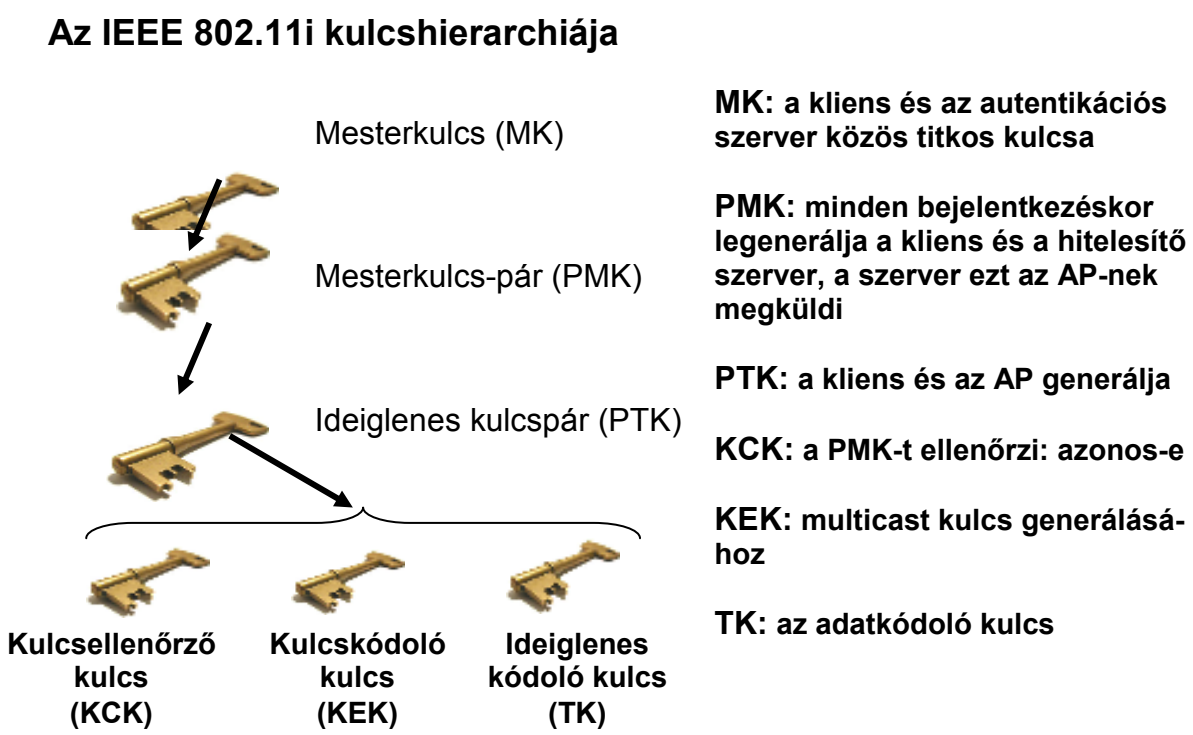
PEAP (Protected EAP):

Az EAP-TTLS és a PEAP között nincs működésbeli különbség, mindössze talán az, hogy a Microsoft és a Cisco áll e módszer mögött, ezért e cégek szoftvereiben (és hardver eszközeiben) ez a beépített funkció található meg. Az EAP protokoll LAN hálózati interfészeken az úgynevezett EAPoL (EAP over LAN) segítségével kommunikál.

RADIUS (Remote Authentication Dial In User Service)

Nem képezi szerves részét az új szabványnak. Az erre vonatkozó ajánlás fő célja az, hogy a vezetékes környezetben már bizonyított és jól bevált protokollt WLAN hálózatban alkalmazza. A RADIUS szerver többféle adatbázist (LDAP, SQL variánsok, ORACLE stb.) támogat, melyben a felhasználó adatai (név, jelszó, kulcs, stb.) tárolódnak.

Titkosítás:



10.ábra: az IEEE 802.11 kulcshierarchiája

WPA esetén szükség van mind a címzett üzenetek, mind a globális titkosító kulcsok újrakódolására. Az ideiglenes-integritási protokoll (TKIP, Temporal Key Integrity Protocol)

minden egyes keretben megváltoztatja az egyszeres üzenetküldés titkosító kulcsát, és minden egyes ilyen változtatást szinkronizál a vezeték nélküli ügyfél és a hozzáférési pont között.

A többes üzenetküldési / globális titkosító kulcs esetén a WPA tartalmaz egy lehetőséget a vezeték nélküli hozzáférési pont számára, hogy elküldje a változásokat a hozzá kapcsolódó vezeték nélküli ügyfelek számára. Amíg a 802.11 számára a WEP titkosítás opcionális, addig a WPA számára szükséges a TKIP-t használó titkosítás. A TKIP a WEP-et egy új titkosítási algoritmussal helyettesíti.

A TKIP a következőket nyújtja:

- Ellenőrzi a biztonsági konfigurációt a titkosító kulcsok meghatározása után.
- A címzett üzenetes titkosító kulcs szinkronizált megváltoztatását minden keretnél.
- Egy egyedi indító címzett üzenetes titkosító kulcs meghatározását minden egyes előre megosztott kulcs hitelesítéséhez.

A WEP gyengeségeit felismerve a 24 bites IV helyett 48 bites IV-t használ (~16millió helyett, ~17,5×1012 állapot) mely esetén több mint 15 évig kellene várni, hogy megismétlődjön ugyanaz az IV, 54 Mbps adatsebesség és 1500bit-es csomagméret mellett. Az IV ugyan 48 bit hosszú, de az első 4 bitet ismétlés elleni védelmet szolgál. A nagyobb méretű IV és az ismétlés elleni védelem használatával kiküszöbölhető a „lexikonépítő” támadással történő kulcsszerzés.

Mivel folyamatos a 802.11i bevezetése, ezért került a WEP kiegészítéseként a TKIP a szabványba. A TKIP használatához nem szükséges a meglévő hardver cseréje, mindössze a hardver meghajtó szoftverét (firmware) kell frissíteni mind AP és felhasználói oldalon. A TKIP továbbra is az RC4 titkosítást fogja használni, IV duplikáció nélkül. A TKIP algoritmus szétválasztja a titkosító kulcsot a hitelesítésnél használttal, a hitelesítés folyamata megegyezik a WEP-évl.

A WPA meghatározza az AES (Advaced Encryption Standard) fejlett titkosítási szabványnak, mint opcionális WEP titkosítás helyettesítőnek a használatát. Mivel az AES támogatás nem lehetséges a szoftver frissítésének segítségével, ezért az AES támogatás nem elengedhetetlen a vezeték nélküli hálózati csatolókon és a vezeték nélküli hozzáférési pontokon.

Adatintegritás:

802.11 és WEP esetén egy 32 bites ICV gondoskodik az adatintegritásról. Bár ez titkosított, kriptoanalízissel lehetséges úgy megváltoztatni a biteket, és úgy frissíteni a titkos ICV-t, hogy a címzett észre sem vegye. WPA esetén egy új Michael – nek nevezett módszer határoz meg egy új algoritmust, amely kiszámol egy 8 bájtos üzenetintegritási kódot (MIC) a létező vezeték nélküli hardvereken rendelkezésre álló számolási kapacitásokkal.

WPA2

A WPA2 gyakorlatilag egy időben készült a WPA -val, ezért is van, hogy a legtöbb implementáció egyesítve tartalmazza a WPA/WPA2 protokollok kezelését. Legfőbb különbség a WPA -hoz képest az AES (Advanced Encryption Standard, fejlett kódolási szabvány) kódoló használata a régi RC4 helyett. Ezen kívül bevezették a négy lépéses azonosítási protokollt, ami nagyobb biztonságot nyújt a kapcsolódáskor történő támadások ellen. A WPA2 „hátránya”, hogy nem kompatibilis a régebbi (820.11a,b) eszközökkel, illetve számos olcsóbb „no-name” eszköz sem támogatja.

	WEP	WPA	WPA2
titkosító algoritmus	RC4	RC4	AES
Kulcshossz	40 bit	128 bites titkosítás 64 bites hitelesítés	128 bit
inicializációs vektor	24 bit	48 bit	48 bit
Csomagkulcs	összefűzött	kevert	nem szükséges
adatintegritás ell.	CRC-32	MIC	CCM
Headerintegritás ell.	nincs	MIC	CCM
kulcsmenedzsment	nincs	EAP-alapú	EAP-alapú

11.ábra: WEP, WPA, WPA2 hasonlító táblázat

IEEE 802.11n szabvány

Még nem véglegesítették a 802.11n szabványt, amely a jelen és egyben a jövő évek vezeték nélküli LAN szabványának gerincét képezi. A végleges változat 2009 júniusában várható.

A 802.11n architektúra már a jelenlegi változatában is 4-6-szoros sebességet kínál a 802.11a/b/g rendszerekkel szemben. A várható sebesség ráadásul nemsokára meg fog duplázódni. A 802.11 a/b/g kliensek nagyobb adatátviteli teljesítményt nyújtanak 802.11n hálózatban, mint a sajátjukban. Köszönhető ez az új MIMO (Multiple Input, Multiple Output) architektúrának, amely egy adott hozzáférési pontnál nagyobb területen biztosít ugyanakkora sebességet és sávszélességet.

A 802.11n egyébként kompatibilis a korábbi 802.11 a/b/g szabványokkal, azaz minden eddig vásárolt vezeték nélküli eszköz használható az új 802.11n rendszerben. Ez nem igényel semmiféle szoftver vagy hardverváltoztatást.

A 2,4GHz-es sáv túlterhelt jelenleg, az 5GHz-es viszont kihasználatlan. Ezt használja ki a 802.11n rendszere, amely mindkét sávot egyszerre használja. Az 5GHz tartományban 21 egymást át nem lapoló csatorna (frekvenciasáv) áll rendelkezésre, míg a 2,4GHz tartományban mindössze három. A több száz megabit/s-os adatátviteli sebesség elérése a csatornák dinamikus váltogatásával lehetséges, ezt hívják DFS2-nek (Dynamic Frequency Selection)

Tesztek alapján 40MHz sávszélesség esetén 5GHz tartományban 150Mbps sebességet mértek, vagyis azonos sávszélességet felhasználva 3-4-szer gyorsabb a 802.11n, mint a 802.11 a/b/g. Utóbbi a gyakorlatban 20-50Mbps sebességet produkál. AES titkosítás bekapcsolása esetén valamelyest csökken az átviteli sebesség.

Általában elmondható, hogy a 802.11n teljesítménye 4-szeresen múlja felül a 802.11g-t, és háromszorosan a 802.11a eszközöket. A 802.11 a/b/g kliens jobban viselkedett 802.11n AP környezetében, mint a sajátjában, nagyobb távolságban, nagyobb sebességet tudott fenntartani.

Támadási módok a WLAN hálózatok ellen

Csomag lopás (sniffer)

A támadó célja a hálózati forgalom figyelése. A legáltalánosabb cél ilyenkor felhasználói nevek és jelszavak megszerzése. Wireless hálózat esetén a támadónak a hálózat rádiós hatókörében kell lennie, vagy ezt a hatókört kell kibővítenie egy megfelelő, érzékeny antenna használatával. Az elfogott csomagok alapján lehetősége van a WEP kulcs törésére, és ezek után az adatokhoz ugyanúgy hozzáfér, mint a kódolatlan hálózatoknál. Ha a támadó csak passzív módon figyel, nincs lehetősége a rendszergazdának a támadót észrevennie.

Session lopás

Ez a támadási mód arról szól, hogy egy legális kapcsolatba fertőzött csomagokat bejuttatva a támadó különböző célokat érjen el. A támadó sniffer programmal figyeli a kommunikációt. Ezáltal megszerzi a támadni kívánt állomás összes szükséges azonosítóját (a MAC címet többek között, szükségképpen). Mivel figyeli a forgalmat, pontosan tudja, hogy az áldozat mit csinál. Módosíthatja a kommunikációt azáltal, hogy az áldozat nevében hamis csomagokat ad fel, vagy egyszerűen csak zavarja a kliens forgalmazását.

AP klónozás

A támadónak persze arra is lehetősége van, hogy saját AP elhelyezésével megtévessze a kliens gépeket, és rávegye őket arra, hogy ahelyett, hogy a legális hálózat AP-jához csatlakozzanak, a hamis AP-t használják. Könnyen kivitelezhető a támadás. A támadó AP-ját nem kell rákötni az elosztóhálózatra, hiszen tényleges forgalmat nem akar lebonyolítani, csak a kliens jelszavát szeretné megszerezni. A kalóz AP-t persze fel kell egy kicsit tunningolni, hogy erősebb jelet adjon, mint a lecserélni kívánt AP. Hiszen a lecserélni szánt AP-t sem bántjuk, mindössze elnyomjuk.

A támadó vagy megnöveli a hamis AP rádiójának adóteljesítményét, hogy erősebb jelet produkáljon, mint az igazi, vagy a kliens és az eredeti AP között helyezi el, ezáltal azonos teljesítmény mellett is a hamis AP jele lesz az erősebb. Ha pedig a támadónak lehetősége van az AP-ját rákötni az eredeti hálózatra, akkor teljes terjedelmében elfoghatja a hamis AP-re feljelentkezett kliensek adatforgalmát, így jutva hozzá bármilyen információhoz.

Hozzáférési pont spoofolás (kommunikációs protokoll szimulálás) és MAC sniffelés

A hozzáférési lista elfogadható szintű biztonságot szolgáltat, amikor kellő erősségű azonosítót használunk, de sajnálatos módon nem ez a helyzet a MAC (Media Access Control Address – egyedi hálózati azonosító, LAN-nál IP cím) címek esetében. A MAC címek egyszerűen ellophatóak, még akkor is, ha a WEP engedélyezve van. Azonkívül még, a vezeték nélküli kártyák engedélyezik a MAC cím megváltoztatását szoftveres úton. A támadó használni tudja ezeket az előnyöket azért, hogy egy valódi MAC címet szimuláljon a vezeték nélküli kártya programozásával, és bejusson a hálózatba. A MAC cím hamisítása nagyon egyszerű. Egy csomag-lopó programmal, a támadó találhat egy helyes MAC címet, és ha a vezeték nélküli kártya engedélyezi a MAC cím megváltoztatását, akkor már készen is van.

Ha a támadó a közelben tartja a vezeték nélküli eszközeit, és ha közel van egy vezeték nélküli hálózathoz, akkor megvalósíthat egy spoof támadást. Ehhez be kell állítania egy hozzáférési pontot (támadó jele, ezt sugározza ő) közel a célpont vezeték nélküli hálózatához vagy arra a helyre ahol az áldozat azt hiszi, hogy a vezeték nélküli internet elérhető. Ha a támadó jele erősebb mint a valódi hozzáférési ponté, akkor az áldozat gépe a támadó hozzáférési pontjához fog kapcsolódni, és miközben az áldozat létrehozza a kapcsolatot, a támadó ellophatja a jelszavát, hálózati hozzáférését, azonosíthatja a gépet stb. Ezt a támadást főleg jelszó szerzésre használják.

AP jelszótámadás

Az AP konfigurációs felülete általában bármelyik gépről elérhető. Az AP-ben lévő szoftver gyártástechnikai okokból – nem lehet egy komplett PC-t bezsúfolni az AP-be úgy, hogy versenyképes áron el is lehessen adni – elég szerény. Például nem nagyon tudja sem bekorlátozni az admin felülethez a hozzáférést, sem a nyers erő támadásokat nem képes felismerni. Így kivitelezhető az a támadás is, hogy az AP-t feltörni kívánó támadó egy program segítségével végigpróbálgatja az összes lehetséges jelszót az AP-re. Nyugodtan teheti, mert az AP nem fogja tudni letiltani, mivel nem is veszi észre a brute force kísérletet. Így csak idő kérdése, hogy a támadó bejusson az AP-be, és saját kénye-kedve szerint átállítsa azt.

Jelzavarás (jamming)

A jelzavarás is a szolgáltatásmegtagadásra irányuló támadások közé tartozik. A vezeték nélküli hálózatok frekvenciaugrásos módszert használnak, amivel elvileg kevésbé érzékenyek a zavaró jelekre. Azonban a 2.4 Ghz-es hullámsávban nagyon sok eszköz működik, amelyek felhasználhatók arra, hogy zavarjuk vele a hálózatot. A vezeték nélküli telefonok, a bluetooth eszközök, de a mikrohullámú sütő is ezt a tartományt használja. Ez utóbbinak hasznos felhasználása is létezik, ugyanis az antennák mikrohullámú jelvisszaverő képességét is ezzel szokták tesztelni az amatőr antennaépítők. Ha a támadó talál egy megfelelően erős jelet kibocsájtó eszközt, akkor azzal el tudja nyomni az állomás jelét, így nem fog tudni sugározni. Erős jel esetén még az is előfordulhat, hogy a zavarás a szolgáltatási területen kívülről érkezik.

Man in the middle támadás

Ebben a kategóriában a támadások legtöbbje az ARP (Address Resolution Protocol – cím visszafejtési protokoll; ez rendeli hozzá az IP címet a tényleges, helyi hálózatbeli géphez), vagy a cache megbolondításán alapszik. Alapvetően, az ARP hamisítás az IP és Ethernet protokoll párbeszédek hibáinak kiaknázása. A támadó összeköt egy hozzáférési pontot egy virtuális magánhálózattal, ami hasonló típusú a célpont hálózatéval. Amikor a felhasználó

megpróbál kapcsolódni a valódi szerverhez, a valódi szervert elfedő szerver visszaküld egy kérelmet, a felhasználót a hamis szerverhez vezetve hogy oda kapcsolódjon. Ez a támadási típus elég komplex.

AP alapértelmezett konfigurálási beállításainak használata

- Alapértelmezett jelszó.
  Az AP-k legtöbbje SNMP vagy HTTP protokollon keresztül konfigurálható, és általában egy alapértelmezett jelszó védi ezeket a felületeket az illetéktelen hozzáféréstől, ezzel hamis biztonságérzetet adva a hálózat üzemeltetőjének. Pedig ha egy támadó hozzáfér az AP-hez (HTTP protokoll esetén ehhez elég egy böngésző program), valószínűleg első dolga lesz az alapértelmezett jelszó kipróbálása. Néhány gyártó alapértelmezett jelszava (ez a jelszó egyes gyártóknál típusonként változik, és van, ahol minden terméknél ugyanaz.

- Alapértelmezett SSID.
  A másik nagy gond az alapértelmezett jelszó mellett, hogy az AP legtöbbje alapértelmezettként egy SSID-t is beállít (csak ismétlésképpen: az SSID az a szöveges azonosító, ami a hálózatot azonosítja. SSID megléte esetén a hálózathoz csak akkor lehet hozzácsatlakozni, ha a kliens is tudja az adott hálózat SSID-jét. Szokták még hálózati jelszónak is nevezni. Ha a rendszergazda ezt az SSID-t nem változtatja meg, akkor ismét csak könnyű prédát kínál a hálózatba behatolni szándékozó ismeretleneknek.

WarDriving

A Wardriving az első, és jól ismert módja, hogy használható vezeték nélküli hálózatokat találjunk (értsd, biztonsági hiányosat). Végezhető egy mobil eszközzel, mint pl. egy laptop vagy Compaq iPaq. WarDriving scannelés egyszerű módon végrehajtható: a támadó magával

viszi az eszközöket egy kocsiba, és detektálja a hálózatokat. Amint egy nyitott hozzáférési pontot detektál, a támadó feltérképezi azt.

A WarDrive-hoz szükséges felszerelés: egy vezeték nélküli hálózati kártya (PCMCIA), egy eszköz, hogy megállapítsa, hogy hol tartózkodik (GPRS), egy laptop, vagy bármilyen más, a hálókártyát fogadni képes mobil eszköz, és egy scanner szoftver. A felszerelés beszerezhető, és nem nagyon drága, érdeklődőkben nincs hiány, így az internet tele van azon városok térképeivel, ahol az önkéntesek már feltérképezték a hálózatokat.

WEP támadások

Az RC4 titkosítási módszer több gyenge és támadásra alkalmas ponttal rendelkezik. Az egyik támadási módszer esetén egy egyszerű számjegyes eljárást alkalmaznak a támadók. Az IV csak 24 bites, így csak fix számú olyan permutáció létezik, amit az RC4 az IV-hez fel tud használni. Matematikailag 2^{24} lehetséges IV-kombináció létezik. Ebben az esetben a kliens aktivitásától függően néhány óra, esetleg néhány nap a kód feltörése. A lehetséges IV-k száma korlátos, ami oda vezet, hogy az RC4 kénytelen egy idő múlva mindig ugyanazokat a karaktereket alkalmazni egy adott IV-hez.

Tehát a támadó egy idő után felismerheti az ismétlődő IV-ket. Elég adat rendelkezésre állása esetén, meg tudja határozni az alkalmazott WEP-kulcsot. Ez egy úgynevezett Brute Force támadás, de ez a módszer időigényes más betörési módszerekhez képest. Ennek az az oka, hogy nemcsak 2^{24} csomagot kell jegyzőkönyvezni, hanem ennek többszörösét.

Egy másik támadási módszer azon alapszik, hogy léteznek ismert, gyenge IV-k. Ez az RC4 természetéből fakad. Az RC4 algoritmus egyes karakterekkel egyszerűen jobban működik, mint másokkal. Ebből származnak a gyenge 24 bites karakterek, de ezeket is felhasználja. Ha tehát ilyen gyenge karaktereket használnak, akkor a támadó néhány algoritmuson át tudja szűrni a lehallgatott adatokat és így képes meghatározni a WEP-kulcs részeit. Ez az eljárás egyik ismert implementációja 10-15 millió csomagot igényel a WEP-kulcs megtöréséhez. A kód megfejtése itt is hasonló módon néhány óra, esetleg néhány nap.

Ingyenes szoftverek az világhálón

Az interneten némi keresgélés után találhatunk ingyenes szoftvereket, amelyek „segíthetnek” minket a vezeték nélküli hálózatok feltörésében.

Ilyen programok például:

- Airodump: alkalmas a WiFi hálózat felderítésére és lehallgatására.
- Aireplay: feladata a csomagok elfogása és hálózatba való visszaküldése. Ezzel az eszközzel lehet forgalmat generálni egy hálózatban.
- Aircrack: a WEP kulcs feltörésére alkalmas szoftver
- Kismet: a hálózat feltérképezésére szolgáló alkalmazás
- Airforge: deautentikációs kérés küldése az AP felé
- AirSnort: WEP kulcsok megfejtésére alkalmas
- WEPCrack: WEP kulcsok megfejtésére alkalmas
- cowpatty: WPA jelszó feltörése brute force módon

Egyszerű veznélküli hálózatok összeállítása

Access Pointok / Routerek elhelyezése

Talán furcsa, de ez is a biztonsági kérdésekhez tartozik. Bárhol is helyezzük el vezeték nélküli állomásunkat a lakásban, irodában, valamelyest mindenképp ki fognak jutni az általa kibocsátott jelek a falakon, ablakokon keresztül. Érdemes azonban úgy megválasztani a helyét, hogy az általunk fontosnak tartott pontokon, a kívánatos rálátás megőrzése mellett, lehetőleg az épület közepe táján helyezkedjen el az AP. Így hatósugarának kültérre eső részét képesek vagyunk minimalizálni.

Sokan egyszerűen közvetlenül a kábel-, DSL modem mellett helyezik el, ami rendszerint nem egyezik az épület középpontjával. Ez a pont sokkal inkább a bejövő kábel-tv vagy a telefonvonal mellett található, és inkább az épület valamelyik külső falánál helyezkedik el. Ebben az esetben a lakás másik végén már meglehetősen gyenge lesz a jel, hála a közfalaknak, kívül az utcán pedig sokkalta erősebb annál, mint az kívánatos lenne. Ne felejtsük el, nem nyilvános internetelérést kívánunk szolgáltatni az arra járóknak!

Az adminisztráció jelszava

Az Access Pointok és Routerek gyári SSID elnevezéssel és jelszóval kerülnek a boltokba, ez minden eszköz felhasználói kézikönyvében szerepel, sőt sokszor az adminisztrátori felület bejelentkező oldalán is megjelenik a gyári beállítás jelszava, ami legtöbbször az "admin" szó. Nyilvánvaló, ha ezt nem változtatjuk meg, ingyen belépőt osztogatunk azoknak, akiket egyébként nem szeretnénk beengedni rendszerünkbe. Első dolgunk legyen a Router vagy Access Point beüzemelése után megváltoztatni az adminisztrátori jelszót! Hosszú (minimum 6 karakternyi), kis/nagybetűk és számok kombinációjából álló kódszót adjunk meg. Létezik sok ingyenes jelszógeneráló kis alkalmazás, amely elérhető az interneten.

SSID

Ahogy az imént is említettük, minden vezeték nélküli AP és Router a gyári beállításokkal kerül a boltokba, ennek értelmében az egy gyártó által piacra dobott termékek ugyanazzal az SSID-val kerülnek ki a gyárból, az SMC például "smc" SSID-val adja ki termékeit, a LinkSys "linksys" SSID-val.

Szintén első teendőink között szerepeljen a gyári SSID megváltoztatása, azonban ezt is megfelelő körültekintéssel tegyük! Semmiképp ne válasszunk olyan szót, amely utal nevünkre, cégünk nevére, az utca nevére vagy bármilyen könnyen hozzánk kapcsolható információra, még a kutyánk nevére sem. Legjobb, ha legalább 6-8 betűből és számokból álló kombinációt adunk meg, ahogy azt jelszó választáskor is tesszük. Az SSID minden egyes adatcsomagban utazik a hálózaton, hogy azonosítani lehessen, melyik AP-tól származik a csomag, egy "krixkrax" SSID is nehezíti valamennyire a betörő dolgát!

SSID Broadcast

Az SSID Broadcast funkció az SSID "szétkürtölését", szétszórását jelenti az AP hatótávolságában. Fontos, hogy a mi eszközeink sem fogják automatikusan megtalálni a hálózatot anélkül, hogy külön megadnánk nekik az SSID nevét, a továbbiakban viszont a kapcsolódás már gördülékeny lesz. A hálózat alapvető funkcióinak beállítása után kapcsoljuk ki, így az átlag kíváncsiskodó nem is sejti majd, hogy vezeték nélküli hálózat van a közelben.

MAC cím szűrés

Ahogy a Routerek beállításaiban általában találkozunk vele: MAC Address Filtering. A MAC (Media-access Control, Eszköz Hozzáférés Ellenőrzés) szűrés annyit jelent, hogy csak azt engedjük a hálózathoz kapcsolódni, akinek az azonosítója szerepel a listánkban. Ez olyan, mintha csak névre szóló meghívóval mehetnénk be egy rendezvényre.

A MAC cím minden egyes termék esetében egyedi a világon, minden gyártó az általa gyártott termékekhez kap egy hivatalosan igényelt azonosító listát, amelyet "beleéget" az adott termékbe, hogy az egyedileg azonosítható legyen. Biztonsági intézkedéseink egyik könnyen alkalmazható és javasolt módszere ez, azonban nem jelent teljes védelmet: ügyes kalózok a

MAC címet is tudják hamisítani, sőt több termék esetében mi is átállíthatjuk, megfelelő alkalmazások segítségével.

Esetenként körülményes lehet ennek a funkciónak a használata, például ha egy barátunk gépét szeretnénk ideiglenesen beengedni a hálózatra, ha átugrik hozzánk néhány dokumentumért. Ilyenkor be kell lépnünk a Router adminisztrációs felületébe, ott rögzíteni a MAC listába a gép azonosítóját, majd ha már nincs rá szükség kitörölni onnan. Mindezek ellenére a MAC cím szűrést javasolt használni.

IP cím tartomány, IP kiosztás és DHCP

A hálózatunkat alkotó eszközeinknek, legyenek azok AP-ok, Routerek vagy számítógépek, mindnek szüksége van egy-egy egyedi azonosítóra, amellyel hivatkozhatnak egymásra a kommunikáció során.

Ez a szám az IP cím, amelyet négy, egyenként 0-255 intervallumból választott számmal adunk meg. A világ összes hálózatán minden egyes eszköz ezen a módon azonosítja magát. Az általunk vásárolt Routerek gyári alapbeállítása általában a 192.168.0.xxx, 192.168.1.xxx vagy a 192.168.2.xxx tartományra van állítva. Az említett konkrét tartományok a "saját alhálózat" szabadon használható tartományai. Ha változatlanul hagyjuk a gyári beállítást, leegyszerűsítjük a betolakodó dolgát.

A DHCP (Dynamic Host Configuration Protocol, Dinamikus Kliens Konfiguráló Protokol) Lényege, hogy egy kliens gép a hálózathoz kapcsolódás elején kérést küld a DHCP szolgáltatást futtató eszköznek: adja meg neki automatikusan a kapcsolódáshoz szükséges beállításokat (IP címet, alhálózati maszkot, átjáró (Gateway) és DNS címeket). Nagy számú hálózati eszköz esetén igen csak segítségünkre van ez a funkció (nem kell minden egyes eszközt egyenként konfigurálni, átkonfigurálni). Azonban otthoni / kisirodai használat esetén javasolt a kikapcsolása: ne kínáljuk tálcán a beállításokat, IP címet az illetéktelen behatolónak, miután esetleg sikerült átjutnia az egyéb biztonsági vonalakon.

WEP

Sajnos már bizonyítottan nem megfelelő technika hálózatunk védelmére, ennek használata önmagában tehát nem javasolt. Számos könnyen elérhető szoftver van, amely alkalmas a WEP kulcsok megfejtésére (AirSnort, WEPCrack).

WPA

A WPA két működési módban alkalmazható.

- Az egyik a Pre-Shared Key mode (Megosztott kulcs mód),
  amely otthonra és kisvállalkozások számára ideális megoldás. A titkos kulcsot az AP adminisztrációs felületén kell megadnunk, ahogy az egyes klienseknél is. Ez első pillantásra megegyezik a WEP módszerével, a WPA azonban a kapcsolódást követően folyamatosan változtatja a titkos kulcsot, így szinte lehetetlen az éppen érvényben lévőt megfejteni. Újabb kapcsolódás esetén ismét az eredeti kulcsot kell megadni, tehát csak arra kell figyelnünk, hogy titkos kulcsunkat senki ne ismerje meg rajtunk kívül. Ezután válasszuk a TKIP vagy AES algoritmust a titkosításhoz, de előtte győződjünk meg arról, hogy eszközeink melyik algoritmust támogatják! Majd adjunk meg egy hosszú, kis/nagybetűkből és számokból álló kulcsot, amit majd a kliens gépek konfigurálásakor is meg kell adnunk. Utolsó beállításként pedig határozzuk meg, milyen időközönként cserélje le az érvényben lévő kulcsot az AP.

- A WPA másik működési módja az Enterprise mode,
  amely nagyvállalatok számára nyújt biztonságos megoldást, otthoni implementálása meglehetősen körülményes. EAP protokolt (Extensible Authentication Protokol, Kiterjeszthető Hitelesítési Protokol) használ a kliensek azonosítására és 802.11x biztonsági szabványt a kliens eszközökön. Az Enterprise mode továbbá alkalmas többszintű felhasználói jogosultság kezelésére is, azaz meghatározható, hogy a hálózaton ki milyen erőforrásokhoz fér hozzá, például ki éri el csak az internetet és ki érhet el egyéb információkat is.

Firmware frissítés

Minden AP és Router, továbbá kliens eszközeink is beépített szoftvert tartalmaznak, amely a hardver lehetőségeit használva valósítja meg a kommunikációt más eszközökkel.

Mivel szoftverről van szó, amelyet emberek, programozók készítettek, természetesen előfordul, hogy valamilyen hibát, biztonsági rést hagytak benne, amelyet kijavítva, illetve egyéb új funkciókkal, szabványokkal kiegészítve a későbbiekben ki szokott adni a gyártó. Ez a firmware frissítés, amit rendszerint letölthetünk a Router vagy AP gyártójának honlapjáról és egyszerűen telepíthetjük eszközünkre. Az említett biztonsági rések, hibák miatt a frissítéseket rendszeresen kell ellenőrizni, és ha újabb jelent meg, mielőbb feltelepíteni, mert az ismert hibákat kihasználva a rosszindulatú behatolók bejuthatnak rendszerünkbe, hiába vérteztük fel hálózatunkat a többi ismertetett biztonsági technikával.

HotSpotok

A hotspot-ok száma rohamosan növekszik, egyre több publikus helyen (éttermekben, kávézókban, intézményekben, stb.) férhetünk hozzá ingyen vagy minimális összeg ellenében az internethez. Óvatosságra kell, hogy intsen azonban minket a tudat: ezek a vezeték nélküli elérési pontok rendszerint nélkülöznek mindennemű biztonsági óvintézkedést az egyszerű tűzfal beállításokon kívül (sőt sokszor még azt is), hogy felhasználóik minél egyszerűbben, problémamentesen kapcsolódhassanak a telepített AP-hoz.

Van néhány fontos óvintézkedés, amit érdemes betartanunk, ha hotspot-hoz szeretnénk kapcsolódni. Mindenképp telepítsünk gépünkre valamilyen tűzfal programot. Tiltsunk le minden nyomtató- és fájlmegosztást a csatlakozás előtt, és ne feledjük: az adatforgalmunk valószínűleg teljesen titkosítás mentes, tehát ha egy szakavatott "érdeklődő" lehallgatja forgalmunkat, abból értékes információkat, bejelentkezési azonosítókat, jelszavakat szerezhet. Amennyiben lehetséges használjunk VPN (Virtual Private Network, Virtuális Magán Hálózat) szoftvert a távoli kapcsolat létrehozására céges hálózatunkhoz. Legyünk tehát rendkívül óvatosak!

Melyiket válasszam?

Az igazat megvallva nem az a kérdés, hogy melyik lehetőséget válasszuk, hanem az, hogy mely lehetőségek kombinációival éljünk WiFi hálózatunk védelme érdekében. Hiába használjuk önmagában például az imént ismertetett WEP technikát a titkosításhoz, ha az illetéktelen behatoló az adatforgalom elemzésével megtalálja a bejelentkezéshez szükséges adatokat. Hiába kapcsoljuk ki az SSID Broadcast-ot, ha nem változtatjuk meg az AP gyári elnevezését, mert egy kíváncsiskodó első próbálkozása valószínűleg pont a gyári nevek végigpróbálgatása lesz, és így tovább.

Általánosságban elmondható, hogy minél több rétegű a védelmünk, annál nehezebb dolga van annak, aki illetéktelenül szeretné használni hálózatunkat és annak erőforrásait.

Összefoglalva, ha betartjuk a következő felsorolt előírásokat, biztonságban tudhatjuk vezeték nélküli hálózatunkon elérhető adatainkat:

- Helyezzük el a lakás megfelelő pontján AP-kat
- Frissítsük AP-nk, Router-ünk és egyéb WLAN képességgel rendelkező eszközünk firmware -jét
- Változtassuk meg az AP-nk adminisztrációs felületéhez tartozó jelszót nehezen kitalálható, megfelelően hosszú kulcsszóra
- Változtassuk meg hálózatunk SSID-jét nehezen kitalálható, megfelelően hosszú kulcsszóra
- Kapcsoljuk ki az SSID Broadcast-ot, hogy ne láthassa illetéktelen az AP –t.
- Állítsunk be MAC cím szűrést, megadva a listában eszközeink MAC címét
- Kapcsoljuk ki a DHCP szolgáltatást a Routeren és konfiguráljuk be vezeték nélküli eszközeinket, adjunk mindnek fix IP címet
- Kapcsoljuk be a WPA biztonsági szolgáltatást, válasszuk a TKIP titkosítást és adjunk meg nehezen kitalálható, megfelelően hosszú titkos kulcsszót

Ne feledjük, hogy önmagában egyetlen biztonsági technológia sem nyújt elegendő védelmet, azonban egyetlen egy alkalmazása is több a semminél!

Összefoglaló

Szakdolgozatomban célja a vezeték nélküli helyi hálózatok alapjainak ismertetése után, ezen hálózatoknál előforduló biztonságtechnikai hiányosságok feltérképezése és a lehetséges védelmi módszerek bemutatása volt. Mivel napjainkban a vezeték nélküli hálózatok egyre nagyobb teret nyernek.

A vezeték nélküli hálózatok nagy előnye az eszközök, s ezzel a felhasználók mobilitásának támogatása, 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. Privát adataink védelme nagyon fontos feladat, főleg cégek, vállalkozások esetében. Persze feltörhetetlen, kijátszhatatlan védelem soha sem létezik, de mindent meg kell tennünk, hogy ez a lehető legnehezebb legyen. Általánosságban elmondható, hogy minél több rétegű a védelmünk, annál nehezebb dolga van annak, aki illetéktelenül szeretné használni hálózatunkat és annak erőforrásait.

Végezetül szeretnék megmutatni egy statisztikát, amely Budapest utcáin készült, és azt bizonyítja, hogy hiába a különböző védelmi technikák, ha nem alkalmazzuk őket.

896 megvizsgált hozzáférési pont közül,

- 176 WPA2
- 222 WEP
- 498 nyitott
- 51 default !

Irodalomjegyzék

Andrew S. Tanenbaum: Számítógép hálózatok

Joseph Davies: Deploying Secure 802.11 Wireless Networks with Microsoft Windows

Addison Wesley: Real 802.11 Security: Wi-Fi Protected Access and 802.11i

Syngress: Hackproofing Your Wireless Network

Syngress: Wireless hacking: project for WiFi Enthusiasts

Chris Hurley, Michael Puchol: WarDriving: Drive, Detect, Defend

Jahanzeb Khan, Anis Khwaja: Building Secure Wireless Networks with 802.11

http://www.wi-fi.org/brand_usage.php

http://en.wikipedia.org/wiki/802.11

http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm

http://www.ieee.org/portal/site

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

http://www.linuxforum.hu/index.php?topic=26673.0

http://www.hoc.hu/forum/index.php?showtopic=1339

http://techline.hu/kiprobaltuk/20071001_wifi_ingyen_kismac.aspx

http://www.wififreespot.com/europe.html

http://www.wi-fitechnology.com/