Szakdolgozat

Tóth Enikő

Debrecen

2010

Debreceni Egyetem

Informatikai Kar

Információ Technológia

Tanszék

Vezeték nélküli hálózatok biztonsága

Témavezető:

Dr. Krausz Tamás

egyetemi adjunktus

Készítette:

Tóth Enikő

mérnök informatikus (Bsc)

Debrecen

2010

Tartalomjegyzék

1. Bevezetés

Napjainkban a leginkább fejlődő iparág a számítástechnika. Igen nehezünkre esne találni olyan háztartást, ahol nem bújik meg a sarokban egy asztali számítógép vagy esetleg egy notebook. Egyre több helyen és alkalmazási környezetben megjelenő eszközök közötti kapcsolat kiépítésre már nem csak kizárólag fixen telepített vezetékes hálózatokat alkalmaznak. A vezeték nélküli hálózatok igénye a mobil eszközök elterjedésével (netbook, notebook, PDA, telefon, stb.) arányosan nő.

Az egyre növő helyi, otthoni, vállalati hálózatokhoz csatlakozni kívánó egyre több felhasználó miatt irodákban, kollégiumokban átláthatatlan lenne a kábel rendszer, melynek karbantartása, továbbfejlesztése egyre bonyolultabbá válik. Ilyen esetekben mindenképpen egyszerűbb vezeték nélküli hálózatot kiépíteni. Mint minden rendszerben itt is voltak elég nagy korlátok, például egy Wi-Fi hálózat átviteli sebessége nem érte el a vezetékes kapcsolatét. De a folyamatos fejlesztéseknek köszönhetően ez a probléma mára már megszűnni készül. Előfordulhat olyan eset is, hogy valamilyen okból nem lehetséges vagy nem praktikus a kábelhálózat kiépítése (pl.: repülőtér), Illetve egyre szaporodik a nagyvárosok vezeték nélküli hálózati pontok száma.

A vezeték nélküli technológia lehetővé teszi, hogy bármikor elérhetővé válik az internet, természetesen csak abban az esetben, ha rendelkezésre áll valamilyen WLAN eszköz, és vezeték nélküli kapcsolat. Hatalmas előnye az eddig megszokott kábeles hálózatokkal szemben, hogy csak részben igénylik a kábeles kiépítést.

A WLAN hálózatok technológiák terjedésével azonban egyre nagyobb igény mutatkozik az adataink védelmére, illetéktelen felhasználók távol tartására. A hagyományos vezetékes hálózat egyértelmű kontrollálhatóságával szemben, hiszen ott csak fizikai kábellel tudtunk csatlakozni a számítógépes hálózathoz. A WLAN hálózatok esetében megfelelő biztonsági módszerekkel tudjuk elérni, hogy csak azok kapcsolódhassanak a hálózatunkhoz, akiknek ténylegesen joguk van hozzá. Ha még nincs felvértezve semmiféle biztonságtechnológiai megoldással, bárki számára elérhető. Aki rendelkezik, vezeték nélküli eszközzel hozzáférhet erőforrásinkhoz, mappáinkhoz, email-jeinikhez stb., amely eddig a vezetékes hálózatunkban-biztonságban tudtuk. Szakdolgozatommal ezekre a problémákra és megoldásokra próbálom

felhívni a figyelmet. Egy kis odafigyeléssel, mennyivel nagyobb biztonságban érezhetjük adatainkat. Folyamatosan születnek megoldások a problémákra, melyek részben vagy egészben nyújtanak megoldást a problémákra. Jelen időkben a szakértők a vezeték nélküli hálózatokat biztonsági szempontból sebezhetőnek tartanak, teljesen jogosan.

Mivel a hitelesítés szorosan összefügg az alkalmazott biztonsági protokollokkal azokat is megvizsgálom (jelenleg a legelterjedtebb a 802.11g és 802.11i szabványban előírt protokoll).

Szakdolgozatomban a hangsúlyt a titkosítási lehetőségekre helyezem. Megpróbálok bemutatni néhány apró eljárást, amelyekkel biztonságosabbá tehetjük Wi-Fi hálózatunkat. Természetesen ez a szakdolgozat terjedelméből is kifolyólag nem fedi le az össze titkosítási és biztonsági kérdést, de megpróbálok minél nagyobb betekintést adni ebbe a témába.

2. Vezeték nélküli hálózatról röviden

A WLAN az angol Wireless Local Area Network szó rövidítése, melynek jelentése vezeték nélküli helyi hálózat, amit leginkább a „vezeték nélküli hálózat”, Wi-Fi és a WLAN névvel illetnek. A WLAN működése hasonló a LAN hálózatokéhoz, csak a jelek más közegben terjednek. Míg a LAN, vezetéket használ (hálózati kábel), addig a WLAN a levegőben továbbítja az információt. Teljes szabadságot és mobilitást biztosít. Jelenleg a jelek sugárzásának esetében nincs bizonyíték arra vonatkozóan, hogy bármiféle egészségkárosító hatása lenne, akár csak a mobiltelefonok esetében sincs.

Megfelelő és helyes beállítások mellett egy Wi-Fi hálózat használata ugyanolyan egyszerű, mint a vezetékes hálózatoké. Ennek oka, hogy a számítógépen elmentett beállítások lehetővé teszik, hogy a számítógép elindítását követően automatikusan csatlakozzon a megfelelő hálózathoz, minden gombnyomás és egyéb művelet nélkül. Egy nagyobb otthoni vagy irodai hálózat kiépítésénél, mindenképpen költséghatékonyabb ez a fajta beruházás, mint a hagyományos helyi házatok, emellett mára már ugyanazt a megfelelő adatátviteli sebességet és kellő odafigyeléssel ugyanazt a megbízhatóságot is biztosítja.

Nem leszünk helyhez kötve számítógépünkkel, így internetezhetünk a folyosóról, az irodánkból, de akár még a kertből is. Nem kell bajlódnunk a sok kábellel, és azért aggódnunk, hogy lesz-e hálózati kábel a közelben!

A vezeték nélküli hálózatokat sok helyen lehet alkalmazni. Az egyik legelterjedtebb alkalmazás a hordozható iroda. Az úton levő emberek gyakran szeretnének a saját kis hordozható elektronikus eszközükkel telefonálni, faxot vagy elektronikus levelet küldeni, távoli fájlokat elolvasni, bejelentkezni egy távoli gépre stb., és ezt akár a tengerről, akár egy repülőgépről is szeretnék megtenni.

Egyik legjobb példa a folyamtatos vezeték nélküli hálózatok növekedésére. A Budapesti Műszaki Főiskola által végzett felmérés alapján betekintést nyerhetünk milyen méretekben is nő a vezeték nélküli hálózatok száma napjainkban. A vizsgálat ugyanazon a 16km-es útszakaszon Budapest egyik külső kerületi útvonalán történt 2004-ben, amely 154 db vezeték nélküli aktív hálózati eszköz talált. Ugyanezen vizsgálat 2009-ben, már 579 db aktív hálózati eszközről árulkodik.

2.1. A WLAN működése

Szükség van vezeték nélküli hozzáférési pontra AP (Acces Point), amely egy vezetékes LAN hálózathoz csatlakozik, amelyek támogatják a biztonságos hitelesítést (hogy csak a megfelelő személyek férjenek hozzá a hálózathoz) és a titkosítást (hogy mások ne lophassák el adatainkat, jelszavainkat). A felhasználó számítógépében szükséges egy vezeték nélküli hálózati kártya. Feladata a vezeték nélküli szakasz kommunikációjának felügyelete, vezérlése és a forgalom továbbítása, elektromágneses jelek sugározásával.

Általában a Wi-Fi hozzáférési pontok szabadtérben kb. 300m-es, zárt térben 50m-es hatótávolsággal rendelkeznek.

Előnyök és hátrányok

A fontosabb előnyös szempontok:

- A számítógépeket könnyű mozgatni, mivel nincsenek kábelek.
- Könnyedén kihasználhatók a nyilvános WLAN-hálzatok.
- A vezeték nélküli hálózatokat általában egyszerűbb telepíteni, mint a klasszikus Ethernet hálózatokat.
- Bővíthetősége az elosztott rendszerek rugalmassága miatt is egyszerűbb, időben is gyorsabb.
- Kezdeti beruházásra van csak szükség, de ez hamar megtérül.

A fontosabb hátrányos szempontok:

- Kevésbé biztonságos, mint vezetékes elődje. Az antennák jelei bárki által foghatóak. A titkosítási módszerek meggátolhatják a lehallgatást.
- A vezeték nélküli hálózatok drágábbak és gyakran lassabbak, mint a klasszikus Ethernet rendszerek.
- Hatótávolságuk néhol korlátozva van pár méterre.
- A vezeték nélküli hálózatban különböző berendezések interferenciát okozhatnak, például falak, nagy fémtárgyak és csövek. Szintén zavarhatják a vezeték nélküli hálózatokat a használatban lévő vezeték nélküli telefonok és mikrohullámú sütők.
- A vezeték nélküli hálózatok gyorsasága az ideálistól eltérő körülmények között mindössze fele a névleges sebességnek.

2.2. A WLAN szabványok

IEEE szabvány	Megjelenés ideje	Működési frekvrencia (GHz)	Sebesség (jellemző) (Mbit/s)	Sebesség (maximális) (Mbit/sec)	Hatótávolság beltéren (méter)	Hatótávolság kültéren (méter)
Eredeti 802.11	1997	2,4	0.9	2	~20	~100
802.11a	1999	5	23	54	~35	~120
802.11b	1999	2.4	4.3	11	~38	~140
802.11g	2003	2.4	19	54	~38	~140
802.11n	2008	2.4/5	74	248	~70	~250
802.11y	2008	3.7	23	54	~50	~5000

2.2.1. 802.11

Az első WLAN-nal kapcsolatos szabvány a Nemzetközi Távközlési Unió, valamint az IEEE (Instiute of Electrical and Electronics Engineering) nemzetközi szabványügyi szövetség emelte szabvánnyá. Az IEEE 802.11 munkacsoport középpontjában a vezeték nélküli LAN-ok. Ezen belül a 802.11 több kisebb munkacsoportot különböztet meg, melynek mindegyikét egy betűvel különböztetik meg pl.: 802.11b, 802.11g… stb. adatátviteli protokollt. Az OSI két legalsó rétegét, a fizikai és az adatkapcsolati rétegét definiálja. Ezeknek a

munkacsoportoknak a feladata a fejlődő egyedi fejlesztések és változásai az alap szabványtől. 1997-ben jelent meg, és mai napig folytatódik a fejlesztése.

Túl az IEEE-n, egy másik szervezet is „vigyáz” WLAN szabványokra, ez nem más, mint a Wi-Fi Alliance (Wi-Fi szövetség). Az ő minősítésük a biztosíték arra, hogy akármilyen vezeték nélküli hálózati felszerelés kipróbált és bizonyítottan használható más berendezésekkel. Keresse a címkét:

2.2.1. 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 25-30Mbit), viszont a nagyobb frekvenciájú rádióhullámok tulajdonságainak köszönhetően (könnyebben elakadnak a különböző tárgyakban, falakon) hatótávolsága kisebb, mindössze 20-30 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 vagy másolhasson nagy fájlokat anélkül, hogy jelentős sebességcsökkenést érzékelne.

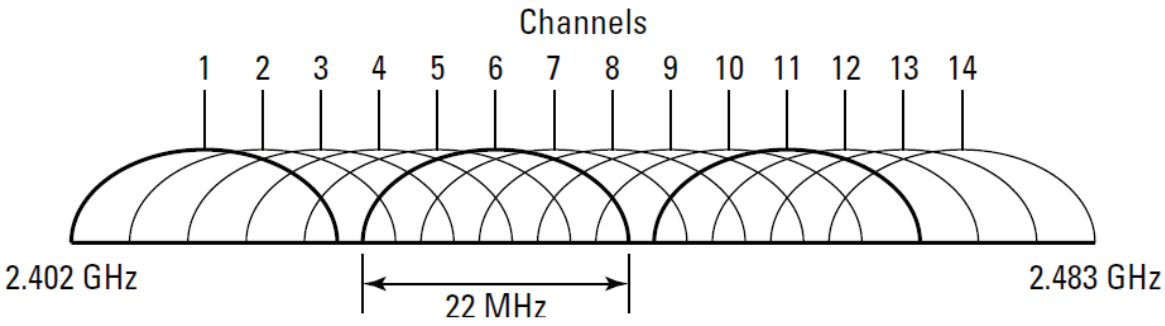
Akkor mi a hátrány? Miért nem használ mindenki 802.11a protokollt? Az ok: a 802.11a nem kompatibilis a 802.11b rendszerrel. A másik ok a hatótávolság, míg a B változat 200 méterig is látható a bázisállomástól addig az A-s hálózaté csak 65-100 méterig tart.

2.2.2. 802.11b

A 802.11 szabvány első revíziója, amely 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 interferálhatnak (zavarhatják egymást). Sávszélességét tekintve 11Mbit/másodperc elméleti maximum adatátviteli sebességre képes, ami a gyakorlatban 4-6Mbit-et jelent. Ez jóval gyorsabb, mint például egy DSL kapcsolat sebessége, azaz bőven elegendő több kliens egyidejű internet kiszolgálására. Komolyabb adatforgalom esetén (zenehallgatás, filmnézés, fájl másolás stb.) azonban már kevesebb lehet. Előnye viszont, hogy már elterjedt és nagyon olcsó, ezért találkozunk vele a legtöbb elektronikai eszközben (telefonokban, PDA-kban stb.). A legtöbb vezeték nélküli LAN 802.11b alapú. Hatótávolsága 30-50 méter épületben, 1 km épületen kívül az AP-ra történő tiszta rálátás esetén.

Ezzel a protokoll rendszerrel maximálisan 14 csatornát használhatunk, az USA-ban csak 11-et. Ez valójában egy viszonylag korlátozott szám, így a csatornák átfedik egymást, kivéve 3-at.

Íme, a jelenség grafikusan:



2.2.3. 802.11g

Az IEEE következő vezeték nélküli szabványa, ugyanabban a tartományban 2,4 GHz-es sávban üzemel, mint a 802.11b, azonban megnövelt 54Mbit/másodperc sávszélességgel rendelkezik. Gyakorlatilag 15-20Mbit-et jelent a valóságban, tehát az ’a’ változattal azonos képességű. A ’b’ változattól ötször annyi adatot lehet küldeni vagy fogadni egyszerre. 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 (ebben az esetben lassul a sebesség). A 802.11g és ’b’ mérnökök ezt szándékosan megengedik.

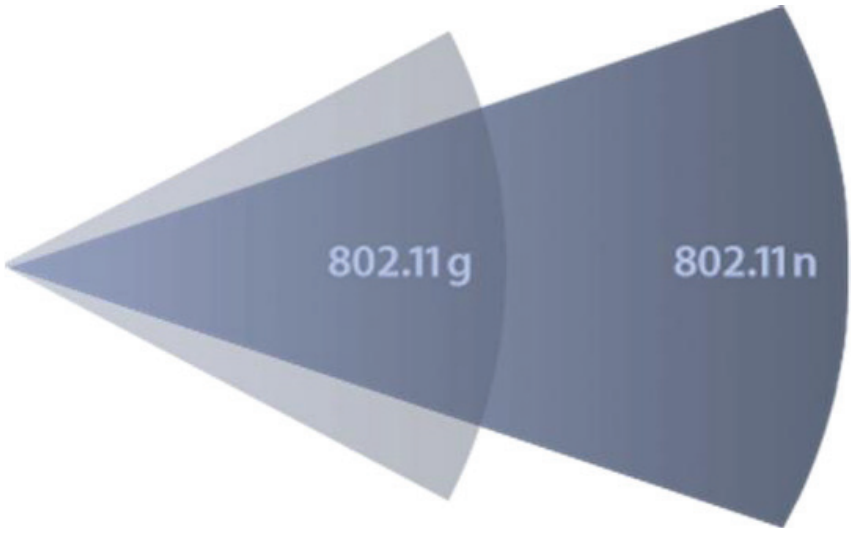
2.2.4. 802.11n

A 802.11n szabványt, amely a jövő évek vezeték nélküli LAN szabványának gerincét képezi. A 802.11n architektúra már a jelenlegi változatában is 4-6-szoros sebességet kínál a 802.11a/b/g rendszerekkel szemben, ami nagyobb, mint 100 Mbps. Érdekesség, hogy a 802.11 a/b/g kliensek nagyobb adatátviteli teljesítményt nyújtanak

802.11n hálózaton belül alkalmaznak egy új architektúrát. Ezt az új MIMO architektúrának (multiple input, multiple output) nevezzük, amely egy adott Access Point-nál nagyobb területen biztosít ugyanakkora sebességet és sávszélességet. A MIMO technológiával az eszközöknek legalább 2 antennája van. Beltéren a legoptimálisabb vételhez a 3 antennás eszközt használják. Az antennákat 45°-os szögben kell beállniuk a felhasználóknak a legnagyobb jelsugárzás eléréséhez. További előnye, hogy kiváló hangminőséget és biztosabb lefedettséget jelent. Emellett a 802.11n képes összekötni a kommunikációs csatornákat, amivel szintén megnő az adatátviteli kapacitás.

A 2,4GHz-es sáv túlterheltnek bizonyult, az 5GHz-es viszont kihasználatlan. Pont ezt lovagolja meg a 802.11n rendszere, amely mindkét sávot egyszerre használja. Az 5GHz tartományban 21 egymást át nem fedő csatorna (frekvenciasáv) áll rendelkezésre, míg a 2,4GHz tartományban mindössze három. A több száz Mbs-os adatátviteli sebesség elérése a csatornák dinamikus váltogatásával lehetséges, ezt hívják DFS2-nek (dynamic frequency selection).

Egy 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.



2.2.5. 802.11i

2004 végén, az IEEE 802.11i a legújabb és a legrobusztusabb biztonsági szabvány. A biztonsági rés betöltésére hozták létre a WPA titkosítási protokollt. Nagymértékben hozzájárul a biztonság javításához, titkosított kulcsokat használnak vagy TKIP (Temporal Key Integrity Protocol) vagy AES (Advanced Encryption Standard) protokollt.

2.2.6. 802.11y

A 802.11y egy szabványosított beavatkozást kerülő protokoll. 802.11y a jövőben áramvonalassá teszi az új frekvenciák örökbefogadását.

Az 802.11y módosítás szintén gondoskodik a káros beavatkozásért. A sávszélesség maximum 54 Mbps lehet, amely az elsődleges felhasználóknak a használt frekvenciája 3,65 - 3,7 GHz-es sáv. Ezen felül különlegesen nagy a hatótávolsága, akár 5 km is lehet

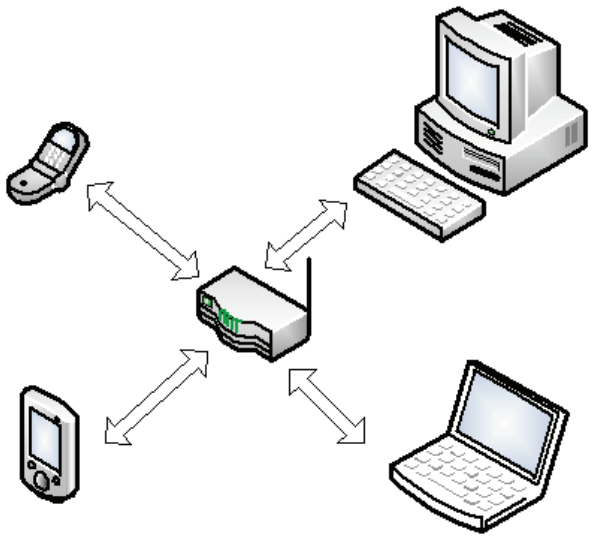
3. Architektúrák

A 802.11-es szabvány meghatároz egy vezeték nélküli állomást (ált. vezeték nélküli hálózati kártyát tartalmazó számítógép). Szükségünk van még egy Acces Point-ra (AP), amely segítségével a vezetékes hálózathoz csatlakozik, és így lehetővé teszi a vezeték nélküli állomás hozzáférését a vezetékes hálózathoz. A hozzáférési pont felügyeli a hálózat forgalmát.

Működésük szerint két eltérő üzemmód szerepel az alapszabványban, és ezt minden vezeték nélküli állomásnak támogatnia kell mindkét működési lehetőséget.

3.1. Infrastruktúramód

Wi-Fi esetében létezik az úgynevezett infrastrukturális mód, amely esetében egy meglévő vezetékes LAN hálózathoz egy vagy több hozzáférési pont csatlakozik, és a vezeték nélküli állomások ezen keresztül kapcsolódnak a vezetékes LAN hálózathoz. Ebben az esetben a vezetékes LAN hálózat kibővül egy vezeték nélküli résszel. Ha a hálózat egy hozzáférési pontot tartalmaz, akkor az üzemmódot alapszolgálatnak vagy központosított módnak (BSS – Basic Service Set) nevezik. A központosított módban működő hálózatok összefoghatóak egy nagyobb struktúrába, melyet bővített szolgálatnak (ESS – Extended Service Set) hívnak. Ebben az esetben a hálózat több hozzáférési ponton keresztül is elérhető. Mindezekre akkor lehet szükség, ha egy állomás nem lát be arra a területre, mint amekkora két távoli vezeték nélküli állomás kommunikációjához szükséges. Az így létrejött rendszert elosztott rendszernek (DS – Distributed System) is nevezik.

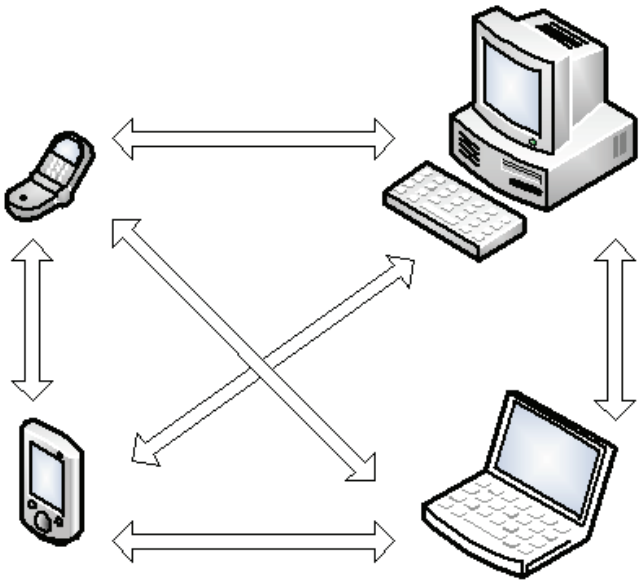


3.2. Ad-hoc mód

A Wi-Fi másik hozzáférési üzemmódját ad-hoc módnak, illetve független alapszolgálatnak (IBSS – Independent Basic Service Set) nevezik. Ebben az esetben a vezeték nélküli állomások közvetlenül egymással (peer-to-peer kapcsolattal) kommunikálnak hozzáférési pont nélkül.

Az üzemmód használatával lehetővé válik a vezeték nélküli állomások számára, hogy hozzáférési pont hiányában is könnyen, hatékonyan és egyéb költségek nélkül létesítsenek egymással kapcsolatot. Ebben az esetben a felügyelő és vezérlő feladatot mindig valamelyik állomás látja el. Ha a kommunikáló felek nem látják egymást, akkor a köztük lévő állomások veszik át az routerek szerepét.

Ha egy kapcsolat felépítésének kezdeményezése során az állomás közelében nincs hozzáférési pont, akkor létrehozhat egy saját IBSS-t, és ez által hozzáférési pontként működhet.



4. A Wi-Fi biztonsága

A vezeték nélküli közeg biztonsága sokkal fontosabb kérdés, mint a vezetékes közegé. Ennek oka, hogy egy esetleges támadónak nem kell közvetlenül hozzáférnie a hálózati csatlakozóhoz, elegendő, ha csak a hálózat hatótávolságában tartózkodik (például ha WLAN hálózat van egy épületen belül, az kívülről is támadható). Sok helyen nem fordítanak rá elegendő figyelmet. A Wi-Fi eszközök általában a lehető legkevesebb biztonsági beállítást

tartalmazzák alapállapotban. Megfelelő védelem (hitelesítő és titkosító protokollok) használatával azonban a Wi-Fi rendszer szinte teljesen biztonságossá tehető.

A vezetékes hálózatok biztonságossá tételére számos lehetőség adódik. Hardveres és szoftveres támogatásra egyaránt létezik hitelesítés, titkosítás és hozzáférés megtagadás. Vezeték nélküli hálózatok esetében nem ilyen egyszerű a dolgunk. A lelakatolt lakásajtónk nem akadályozza meg a rádióhullámok terjedését. Rosszindulatú felhasználók mindig is lesznek, akik a teljes hálózati forgalmat lelophatják anélkül, hogy észre tudnánk venni.

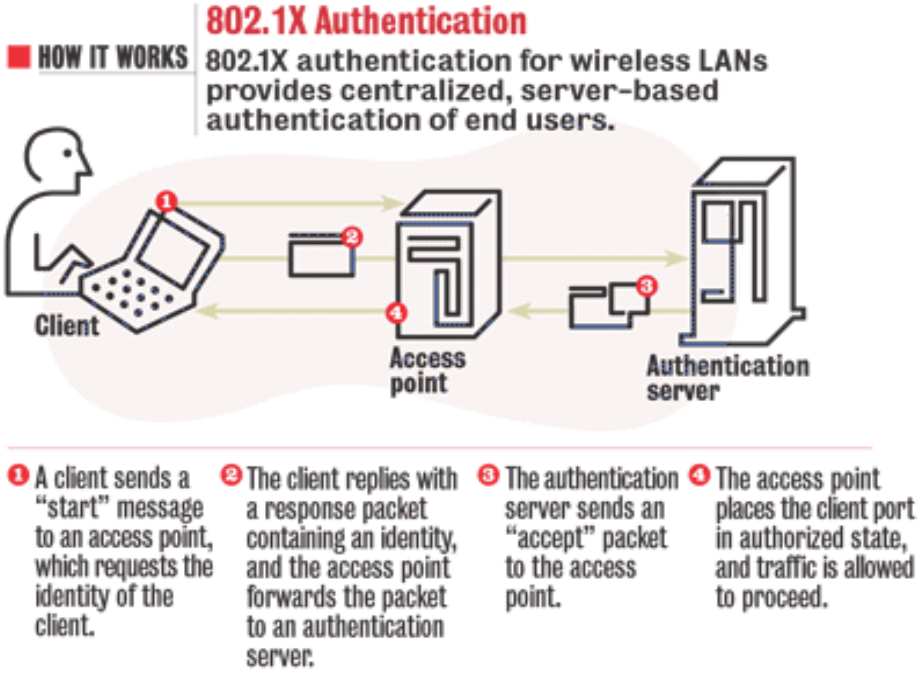
4.1. Hitelesítés

Amikor két protokoll résztvevői kommunikálnak egy biztonságos csatornán (például az Internet, LAN, stb) szükség van arra, hogy a feladó **hitelesítse** magát, és úgy küldjön üzenetet, hogy a vevő meg legyen győződve a feladó személyazonosságát illetően. A szakemberek idővel rájöttek, hogy a megfelelő biztonság elérése érdekében nem kizárólag az eszközöket kell nyílván tartani a hálózatban. A hitelesítő rendszer feladata eldönteni, hogy egy csatlakozni kívánó felhasználó valóban használhatja-e a hálózati erőforrásokat. Vagyis például kapcsolódhat-e az adott Wi-Fi hálózat AP-jához, és használhatja-e a vezeték nélküli hálózat erőforrásait. Emellett létezik üzenethitelesítés is, amely már egy hitelesített viszonyban a titkosított üzeneteket védi a módosítással szemben (integritásvédelem), és lekövethető legyen az az üzenet, ha esetleg egy harmadik személyhez is továbbításra kerül. Tudnunk kell azt is kitől kapjuk az információt és a küldőnek is biztosnak kell lennie abban, hogy a címzett az adatokat megkapja e. Fontos hogy ez az integritás ne sérüljön. Az azonosítót a felhasználótól kapott adattal ne lehessen manipulálni. Erre a problémára használatos a hash függvények segítségével bármely bitsorozatból egy rögzített hosszúságú ellenőrző kódot képezhetünk, amely csak az eredeti bitfolyamra jellemző. A leképezés egyirányú, dekódolás nem lehetséges. Ha egy bitet megváltoztatunk az eredeti üzenetben, akkor a kimenet is mindenképpen változik. Annak a valószínűsége kicsi, hogy két különböző bitsorozatnak ugyanaz legyen a hash értéke. Ez a folyamat sokkal kevesebb időt vesz igénybe. A gyakorlatban leggyakrabban használt hash algoritmus az **MD5** (Message Digest 5),

egy felhasználóneveket és jelszavakat használó, egyirányú hitelesítési módszer. Nem támogatja a kulcskezelést, de adattitkosítás használata esetén előre konfigurált kulcsot igényel. Biztonságosan használható, EAP titkosított csatornán belül, vezeték nélküli hálózati hitelesítésekhez.

Mára már kialakítottak egy biztonsági megoldást a felhasználói alapú hitelesítésre – az **IEEE 802.1X** protokoll segítségével. Amelyben már lefektették a hitelesítési alapokat különböző rendszerek és algoritmusok segítségével. Azt a tényleges algoritmust, amellyel a felhasználó hitelesére használt módot nem rögzítették, ezáltal hitelesítési keretrendszert biztosít különböző hitelesítési és kulcskezelési protokollokhoz. A 802.1X már egy létező protokollt használ, az EAP-t (Extensible Authentication Protocol), amely leírja, hogy működik az Ethernet, a Token Ring, vagy a vezeték nélküli LAN-ok, az üzenetek cseréje során alkalmazott hitelesítési folyamatot.

Az IEEE 802.1X szabványban, a kliens (a könyörgő) hozzáférést kér egy hozzáférési ponttól (hitelesítő). A hozzáférési pont a felhasználónak (a felhasználó kliens szoftver), még ha jogosulatlan is rá lehetővé teszi, hogy küldjön egy EAP üzenetet, felkéri az ügyfelet, hogy azonosítsa magát. Az ellenőrizetlen portok lehetővé teszik az EAP csomagok zavartalan áthaladását a hálózatban. Az ellenőrző port, amely lehetővé teszi az összes csomag megindítását, ha a kliens hitelesítése sikeresen megtörténik (lásd: a lenti ábra alapján). Az ügyfél erre egy azonosító csomaggal válaszol, amelyet a hozzáférési pont továbbküld a hitelesítő kiszolgálónak, amely a saját használt algoritmusával beazonosítja a felhasználót. Ezután a hitelesítő k „elfogadom” csomagot küld vissza a hozzáférési pontnak. A hozzáférési pont elfogadhatja vagy elutasíthatja az üzenetet. Feltételezzük, hogy elfogadják az érkezett hozzáférési pontváltozásokat.



A hitelesítés a második fontos pillére a biztonságos **VPN** (Virtual Private Network) kialakítása. Amely megvédi a rendszert a jogosulatlan felhasználóktól, és az ismétléses támadástól. A virtuális magánhálózat egy olyan hálózat, amely fizikailag több különböző helyi hálózatot fog össze (pl. vállalatok gép hálózatát) a nyilvános hálózatokon (pl. Interneten) keresztül és mindezt úgy teszi, hogy az egyes hálózatok között az adatcsere, és konkrétan a hálózati forgalom biztonságosan zajlik. A VPN megoldások segítségével a VPN ügyfelek kommunikálnak a VPN szerverekkel, amik azonosítják őket. Legnagyobb előnye, hogy képes dolgozni magán és nyilvános hálózatokon is.

Hitelesítési folyamatok:

- Egyirányú

Ebben az eljárásban mindig csak és kizárólagosan az egyik fél végzi el a hitelesítést. Egy vállalatnál vannak kitüntetett kezdeményező és külön válaszadó szerepet betöltött gépek.

- Kétirányú

Itt is az egyik fél minden esetben kezdeményezi a hitelesítést, de nincs előre meghatározott szerepe. A kezdeményező és a válaszadó szerepe felcserélhető és vissza. Ugyanolyan állapotú gép fut kezdeményező és válaszadó módban. Ilyenkor akkor adódhatnak problémák, ha ezek a gépek egyszerre akarják vagy a küldő vagy a válaszadó szerepét.

- Csatolt egyirányú

Két egyirányú forgalmat kell kiépítenie, mielőtt a forgalom elkezdődik. Minden entitás az áramlások alatt veszi fel a kezdeményező és reagáló szerepet is. Mind a kezdeményezője és mind a reagálók gépeket kitüntetett szerepet kapnak, amelyek futnak minden adatmozgásnál.

4.2. Titkosítás

A titkosítás az az eljárása, amellyel az információt (nyílt szöveget) egy algoritmus (titkosítási eljárás) segítségével olyan szöveggé alakítjuk, ami olvashatatlan olyan ember számára, aki nem rendelkezik az olvasáshoz szükséges speciális tudással. Ezt a tudást általában kulcsnak nevezünk. Az eredmény a titkosított információ (titkosított szöveg). A titkosítás habár meg tudja védeni az üzenet bizalmasságát, de szükség van más technológiákra is, hogy biztosítani tudjuk az üzenet sérthetetlenségét és hitelességét. Számos titkosító eljárás egy az egyben (vagy egyszerű átalakítással) használható megfejtésre is, azaz, hogy a titkosított szöveget újra olvashatóvá alakítja.

Az összes Wi-Fi berendezés támogatja valamilyen formában a titkosítást. Titkosítási technológia összekuszálja a küldött üzeneteket a vezeték nélküli hálózaton, így nem olvasható az ember számára. Napjainkban számos titkosítási technológia létezik. A titkosítás biztosítja a lehallgatás mentességet, vagyis megvédi az adatokat az illetéktelenek hozzáférésétől. A tűzfalon felül természetesen más védelmi módszerekre is szükségünk van. Ahhoz, hogy biztonságosan kommunikálhassunk egy nyilvános csatornán, az adatokat

titkosítani kell. Jó néhány algoritmus áll rendelkezésünkre, amelyek az operációs rendszerünktől függetlenül alkalmazhatók. Ezek az eljárások erőforrást és időt igényelnek a rendszerünktől.

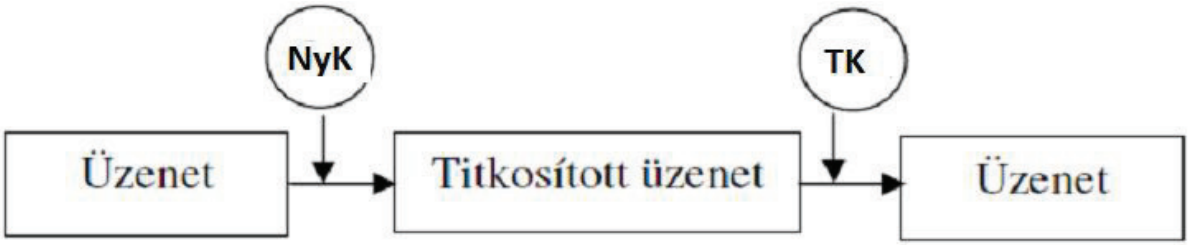
Titkosítási eljárások:

- Nyilvános kulcsú titkosítás

  Ennek a titkosítási algoritmusnak az a lényege, hogy a kódoláshoz és dekódoláshoz különböző kulcsokat használ. Létrejöhet a titkosított kommunikáció, hiszen minden fél ismeri a megfelelő titkos és nyilvános kulcsokat. Ez a módszer nem csak ebben az esetben létezik, több algoritmus használja ezt a módszert, nem utolsó sorban VPN titkosításra is felhasználható. Nehéz kiszámítani a titkos kulcsot. A kulcsok tárolása elég problémás, de a kulcshasználata hosszú életű.

  NyK = Nyilvános kulcs

  TK = Titkos kulcs



RSA titkosítási algoritmus:

Első nyilvános kulcsú titkosítás, amit Rivest, Shamir és Adleman dolgozta ki és nyilvánosságra 1987-ben hozták. A jelenlegi matematikai ismeretek alapján az RSA-titkosítás eredménye nem fejthető vissza elég gyorsan, ezért nem érdemes megpróbálni, bár nem bizonyított, hogy nem létezik kellő gyorsaságú algoritmus a visszafejtésre.

Az RSA algoritmus 3 lépésből áll:

1. termelés,

2. titkosítás és

3. visszafejtés

Válasszunk ki 2 nagy prímszámot: p és q. Ahol

$n = p*q.$

Legyen:

$m = (p – 1)*(q – 1).$

Válasszunk ki egy kis egész számot:

$1 < e < m$ relatív prímet.

Határozzunk meg egy:

$d = e^{-1} \bmod m),$

azaz d a multiplikatív inverze az e mod m- nek.D-t tartjuk, mint nyilvános kulcs kitervőjének.

Titkosítás:

$c = m^{e} \pmod n.$

Dekódolás:

$m = c^{d} \pmod n.$

Példa:

1. p = 61 és q = 53.
2. n = 61 * 53 = 3233.
3. m = (61 - 1) * (53-1) = 3120.
4. e = 17.
5. d = 2753.

Titkosítás: m = 65.

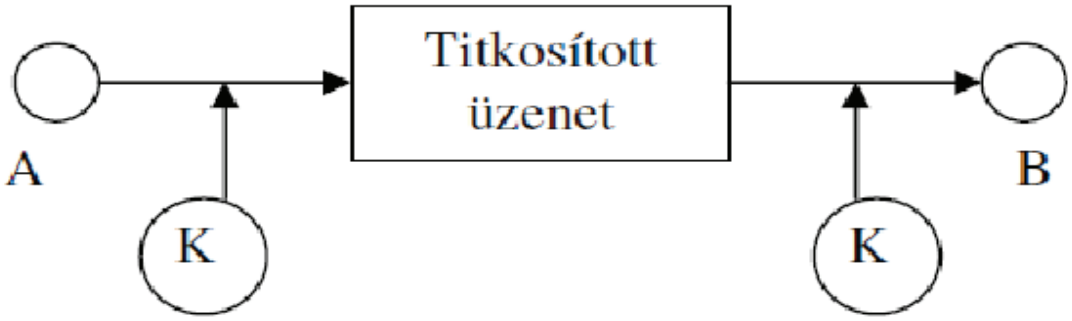
$c = 65\ 17 \pmod{3233} = 2790.$

Dekódolás: c = 2790.

$m = 2790\ 2753 \pmod{3233} = 65.$

- Szimmetrikus kulcsú titkosítás

Ennek a titkosítási algoritmusnak az a lényege, hogy kódoláshoz és dekódoláshoz ugyanazt a kulcsot használják. Ezt csak úgy lehet megvalósítani, hogy a kulcsot mindkét fél ismeri és bizalmasan kezeli. Gyors az algoritmus és valós idejű a titkosítás. Problémás, hogy a kulcsot átvitel előtt át kell juttatni a másik félhez és minden partnernek különböző kulcsot kell rendelnünk. Mindezt úgy, hogy egymás üzeneteit ne lássák.

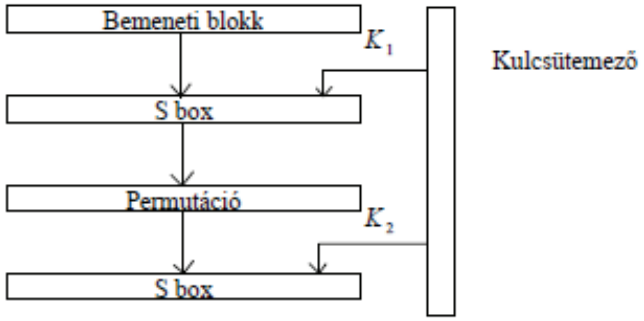


DES titkosítási algoritmus:

Az egyik legelső elterjedt adattitkosítási szabvány a DES (Data Encryption Standard) volt. 1976. IBM szabadalom, egy 64 bites blokk kódoló.

1977-ben lépett a nyilvánosság elé, látszólag 64 bites, effektíven 56 bites titkosítási kulcsokat használt. Minden 8 bit paritásbit. Amely a maga idejében még megállta a helyét, de a számítógépes kapacitás folyamatos növekedésével nem nyújt biztonságot, de még mai napig engedélyezett algoritmus és széles körben használják.

A DES nagy előnye és gyorsasága, hogy pontosan ugyanazt az eljárást használja kódolásra és dekódolásra, csak az algoritmus során felhasznált kulcsrészleteket kell fordított sorrendben „adagolni”. Nagy hátránya a kis méretéből adódóan könnyen és rövid idő alatt feltörhető.



S box : a bemenetéhez a kulcstól függően kimenetet rendel

3-DES titkosítási algoritmus:

Ezt követő módszer a 3-DES nevezetű módszer, amely egymás után háromszor ismétli meg a titkosítást az adatblokkokon.

D_{K1} (kódoló)(D_{K2}^{-1} (dekódoló) (D_{K3}) (kódoló)). 3x56 = 168 bites a kulcs.

K1 = K3 $\rightarrow$ 112bites a kulcs.

1997-ben a DES leváltására, a NIST (Egyesült Államok kormányának a Nemzeti Szabványügyi és Technológiai Hivatal) pályázatot írt ki. A NIST a világ minden tájáról hívott össze kriptográfiai és adatbiztonsági szakembereket, hogy megvitassák és kiválasszák a legmegfelelőbb algoritmusokat. 5 titkosítási algoritmust találtak, amelyek megfeleltek a követelményeknek. A végleges választás egy belga pályázó algoritmusa lett. Ez az algoritmus az EAS (Advanced Encryption Standard) nevet kapta.

EAS titkosítási algoritmus:

2000-ben a NIST hivatalosan is elfogadta az EAS titkosítási szabványt. A belga Vincent Rijmen dolgozta ki. Széleskörű elterjedést és alkalmazást várva tőle. A legújabb szabvány alapján ez az algoritmus felel a vezeték nélküli hálózatok biztonságáért.

2002-ben az IEEE 802.11i szabvány csoport és a Wi-Fi Allience tervezett egy újabb algoritmust TKIP (Temporal Key Integrity Protocol, időváltozás kulcsvédő protokoll) néven.

A WPA2 által használt szabvány. Az EAS algoritmus (Rijndael – algoritmus) a titkosítási kulcsokat blokk titkosítóval valósítja meg, és több lépésben titkosít. A blokk alapú titkosítás

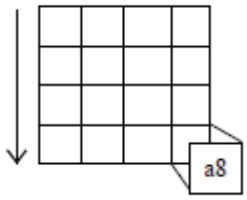
egy olyan algoritmus, hogy egy időben több adatblokkot kezel egyszerre. Egy blokk általában 128 bit hosszú. A több lépés utal arra, hogy az algoritmus keveri az adatokat a titkosítás során, újra meg újra hossztól függetlenül egy adatot többször a „keze alá vesz”. Ugyanazt a titkosítási kulcsot használja az adatok titkosítására és dekódolására.

Az EAS három blokk titkosítási változata:

- AES-128
- AES-192
- AES-256

Az EAS 128 bites fix blokkokat használ, a kulcs mérete lehet 128, 192 vagy 256 bites. A 10 lépéses változata 128 bites, a 12 lépéses a 192 és a 14 lépéses a 256 bites kulcsú változat.

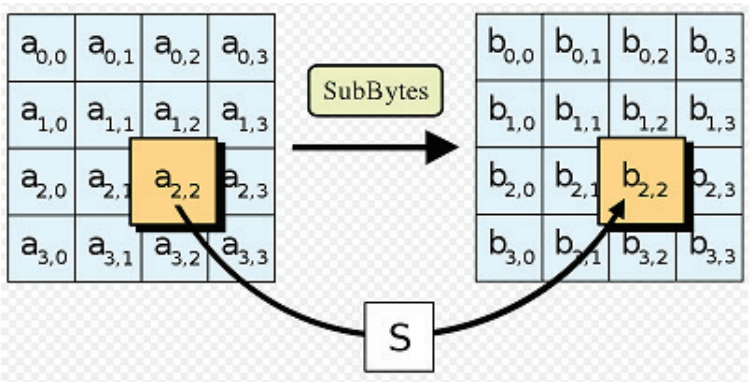
A 128 bitet oszlop folytonosan helyezi el egy 4X4 byteos mátrixban.



Az AES titkosítás 10 ismétléses körből áll, minden körben 4 különböző művelet váltja egymást.

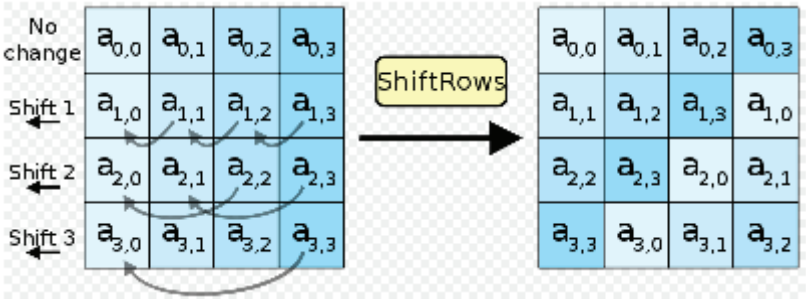
- ByteSub(State);

Az állapot egy byte-ját $a = a_1a_2$, és cseréljük a-t a ByteSub Mátrix a_1-dik sorának a2-dik elemével.



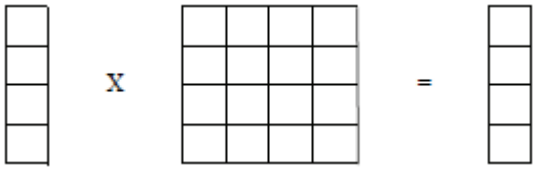
- ShiftRow(State)

Az alapmátrix j-edik sorát balra a j-1-edikre sorra léptetjük az első sor kivételével.



- MixColumn(State)

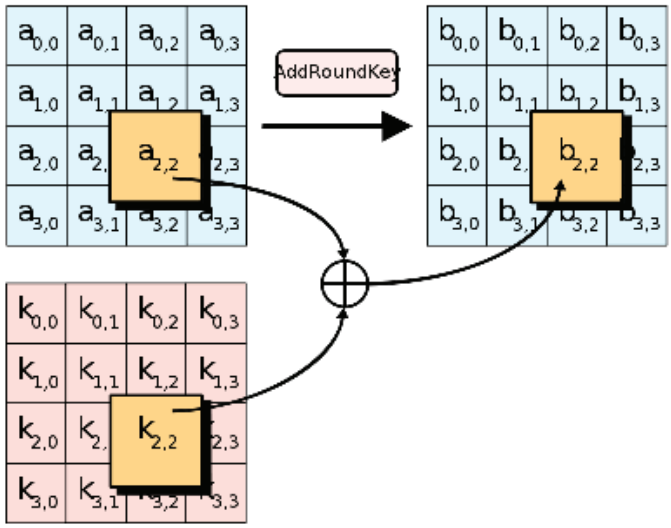
Az alapmátrix i-edik oszlopát megszorozzuk egy előre megadott mátrixszal.



A 10-ik körnél hiányzik ez a művelet.

- AddRoundKey(State)

Az alapmátrix byte-jaihoz bitenként logikai összeadással hozzáadjuk a menetkulcs megfelelő byte-jait.



TKIP titkosítási algoritmus:

A WPA által használt szabvány, mint alapjául szolgáló szimmetrikus kulcsú titkosítási algoritmus. A TKIP egy kicsit kevésbé biztonságos, mint az AES. A főbb különbség, hogy a TKIP-et szoftver vezérli, amíg az AES-t szoftver által vezérlik. A TKIP ugyanazt az RC4 alapú titkosító, ami a WEP-en belül létezik, azzal a kivétellel, hogy a WEP összefűzte a kulcsokat, míg a TKIP összekeverte őket az inicializáló vektor segítségével. Ezzel is bonyolítva a dekódolás bonyolultságát, ami egy támadónak lényegesen kevesebb adatot enged visszafejteni csak egy kulcs használatával. Nem utolsó sorban még végrehajt egy fokozatos számlálást az ismétlődő támadások kivédésére. A csomagokat, amiket üzemen kívül kapott, el fogja utasítani a hozzáférési pont. Végül, a TKIP végrehajt egy 64 bites üzenet sértetlenségi vizsgálatot, amit MICHAEL-nek hívnak.

A TKIP is rendelkezik az „újrakulcsoló" mechanizmussal, amely minden adatcsomagot egy egyedülálló titkosító kulccsal küld el. Minden csomag kap egy egyedi 48 bites sorszámot, amely növekszik minden egyes alkalommal, amikor új csomagot továbbítunk. Ezzel kiküszöbölték az ütközési támadásokat, amik akkor következnek be, ha ugyanazt a két kulcsot használja két csomag.

A TKIP-et nem fejlesztették tovább és a 802.11 szabvány a következő teljes kiadásában hatálytalanítva lett.

4.2.1. WEP

1997-ben az elsőként használt titkosítási protokoll a WEP (Wired Equivalent Privacy, magyarul Kábellel Egyenértékű Titkosság) volt. Eredetileg az IEEE 802.11b hálózatokra fejlesztették ki. DE a 802.11a/b/g szabványok biztonsági rendszere a WEP titkosításon alapul. Bemutatásakor arra szánták, hogy hasonló bizalmas hálózatként működjön, mint egy általános vezetékes hálózat, ahogy erre a neve is utal. Például egy támadó a vezetékes Ethernet hálózathoz akar csatlakozni, akkor hozzá kell férnie az internet megosztóhoz. Mivel azonban a hálózati eszközök általában fizikailag védve vannak (zárt szobában), ezért a

támadó nehézségekbe ütközik. Ezzel szemben egy védelmi mechanizmus mentes vezeték nélküli hálózathoz a hozzáférés triviális feladat. A WEP ezt a triviális feladatot hivatott volt megnehezíteni. Fontos kihangsúlyozni, hogy a szakemberek nem törekedtek a „tökéletes" biztonságra. A WEP jobb, mint a semmi, de mára már egy korszerűtlen algoritmus. Ezen felbuzdulva az IEEE új biztonsági architektúrát dolgozott ki, melyet a 802.11i szabványnak nevezték el.

Működése:

Vezeték nélküli hálózatok esetében két alapvető biztonsági probléma merül fel. Egyrészt a rádiós csatorna jellege miatt a kommunikáció könnyen lehallgatható. Másrészt – ami talán még fontosabb – a hálózathoz való csatlakozás nem igényel fizikai hozzáférést a hálózati csatlakozóponthoz (AP), ezért bárki megpróbálhatja a hálózat szolgáltatásait illegálisan igénybe venni.

A szabványos WEP az RSA Data Security RC4 algoritmuson alapul. Létezik 64, 128, 256 és 512 bites változata is. Legelterjedtebb a 64 és a 128 bites WEP.

A 64 bites, amiből 40 bit a titkos kulcs, amit egy 24 bites inicializációs vektorral konkatenálnak.

A 128 bites WEP kulcs, általában 104 bit hosszú, ehhez adódik hozzá a 24 bit hosszú inicializáló vektor, így jön ki a 128 bites titkosítás.

Több felhasználó esetén minden kliensnek ugyanazt a kulcsot kell megadni.

A WEP az első problémát az üzenetek rejtjelezésével igyekszik megoldani, a második probléma megoldása érdekében pedig megköveteli a csatlakozni kívánó mobil eszköz hitelesítését az AP felé.

A WEP rejtjelező algoritmusa az RC4 kulcsfolyam kódoló. A kulcsfolyam kódolók úgy működnek, hogy egy kisméretű, néhány bájtos titkos kulcsból egy hosszú állandó véletlen bájtsorozatot állítanak elő, és ezen sorozat bájtjait a XOR matematikai művelet segítségével rejtjelezik az üzenet bájtjait. Ez történik a WEP esetében is.

Az egész csomag sértetlenségét CRC-32 algoritmussal védik, ami a csomag megváltoztatása után kicselezhető. Ez egy ellenőrző összeg, amely a nyílt üzenettel együtt kerül titkosításra. Ennek a CRC-nek egyik célja, hogy kizárják a szándékos módosításokat.

Tehát a titkos WEP kulcs, valamint az üzenetenként egyedi inicializáló vektor segítségével előállíthatjuk a hosszú véletlen véletlen sorozatot, majd ezzel és a XOR művelettel titkosítjuk az üzenetet – végül az üzenethez hozzáfűzzük a nyílt inicializáló vektort.

Összesítve az általános WEP elemei:

K: titkos kulcs (40 bit)

IV: inicializáló vektor (24 bit)

CRC-32: (Cyclic Redundance Check) a hitelesség garantálásáért

RC4: kulcsfolyamat generálására

M: a kódolandó üzenet

Kódolás:

$$\underline{WEP(M, IV, K)} = \{IV, [M, CRC(M)] \ \textbf{XOR} \ RC4(IV, K)\} = C$$

A tervezés során elkövetett hibák miatt azonban ez a protokoll nagyon sérülékeny (elsősorban az inicializációs vektor kis mérete miatt). A megfelelő jelerősség esetén nagyon

egyszerűen visszafejthető a WEP kulcs. Néhány egyszerű és ingyenes program segítségével gyorsan megfejthetők.

A WEP hibái

A WEP tulajdonképpen a rossz protokolltervezés mintapéldája.

- A titkosítás csak a kliens és az AP között van, így a beérkezett titkosított csomagot az AP visszafejti, és titkosítás nélkül küldi tovább a vezetékes hálózat felé.
- A hitelesítés egyirányú, a kliens gép hitelesíti magát a hozzáférési pont felé, de a hozzáférési pont nem hitelesíti magát a kapcsolódni kívánt eszköznek.
- A hitelesítés és rejtjelezés ugyanazzal a kulccsal történik, így az egyik megszerzésével már a másikat is tudjuk.
- Miután a hitelesítés megtörtént és csatlakoztunk a hálózathoz, bárki küldhet üzenetet az egyszer már hitelesített kliens nevében, annak MAC címét használva.
- A titkos kulcsot ismerő kliensek olvashatják más gépekről küldött vagy oda beérkező csomagokat. Mivel mindenki ugyanazt a WEP kulcsot használja, így a titkos csomagok bárki által visszafejthetők megfelelő szoftverek segítségével.
- Egyedül a bonyolult jelszó védhet meg jobban minket a támadásokkal szemben.
- A legtöbb AP lehetőséget biztosít MAC vagy IP cím alapján történő szűrésre. Beállítható tartomány, egyedi cím, amivel csatlakozhatunk az eszközhöz.
- Van lehetőségünk még a hackerek dolgának megnehezítésére, bár ez is kijátszható. Kikapcsolható például az AP-ban az SSID (Service Set Identifier) sugárzása, így az egyszerű kliensek nem mutatják magukat meg a lehetséges hálózatok listáján. Ekkor kézzel kell megadnunk az SSID-t, a kapcsolat létrejöttéhez.

Az SSID: a vezeték nélküli hálózatok esetében használatos azonosító, melyet az adatcsomagokhoz kapcsolnak. Ez alapján lehet azonosítani, hogy az adatcsomagok, mely hálózathoz tartoznak. Ezen felül az SSID egy hálózati eszközcsoport azonosítására szolgál.

Maga az azonosító szöveges és alfa numerikus karakterekből állhat és maximum 32 karakter hosszú lehet. Az egy hálózathoz tartozó eszközöknek ugyanazt az SSID-t kell használniuk.

A WEP gyengeségeinek lehetséges kihasználásai

- Passzív támadással, mellyel a forgalmat lehet dekódolni: statisztikai analízis útján deríthető ki a forgalmazott adathalmaz.
- Aktív támadással, melynek során nem hitelesített állomásról szúrnak be új forgalmat: ismert szöveg alapú támadással lehet visszafejteni a forgalmat.
- Aktív támadással, mellyel a forgalmat dekódolják: a támadás az AP-val való „trükközésen" alapul.
- Szótár alapú támadás: az elmentett adatforgalomból utólag szedik ki a WEP kulcsot.

Néhány WEP törési szoftverek Linux alatt:

- Airodump: alkalmas a Wi-Fi hálózat felderítésére és lehallgatására.
- Aireplay: feladata a csomagok elfogása és hálózatba való visszaküldése. Ezzel az eszközzel lehet elfogni az áldozat és a hozzá kapcsolódó router közötti forgalmat, melyekből kinyerhető a kulcs.
- Aircrack: a kulcs feltörésére alkalmas szoftver.

Másodpercek alatt megtalálják a használt kulcsot. A szükséges csomagok akkor is kikényszeríthetőek, ha senki se kapcsolódik a hálózatra vezeték nélkül!

A törés folyamata:

- Felderítjük a hálózatot, azonosítjuk a célpontot.
- Elfogjuk a célpont és a hozzá kapcsolódó kliensek közötti forgalmat, különös tekintettel az ARP csomagokra, melyekből a nyílt szöveg alapú támadással egyszerűbben kinyerhető a kulcs.
- Az elfogott adatcsomagokból brute force módszerrel kinyerjük a kulcsot.

További megvalósított, de nem szabványos hibajavítások

4.2.2. WEP2

Ez a 802.11i első vázlataiban lett megfogalmazva a WEP ráncfelvarrásaként. Futtatható volt azon a néhány hardveren, amely nem volt képes a WPA-t vagy a WPA2-t futtatni és kiterjesztették a biztonsági kulcs értékét 128bit-re. Ez némileg segített a "brute force = nyers erőt" alkalmazó támadások kivédésében.

Mikor már tiszta lett, hogy a teljes WEP algoritmus hiányos (nem csak a kulcs titkosítása miatt) és még több hibajavítást igényel, akkor elvetették az eredeti algoritmust is.

4.2.3. WEPplus

A WEPplus a WEP tovább fejlesztése az Agere Systems által. Ez a cég a WEP biztonságát növelte, elkerülve a "gyenge Inicializáló Vektorokat". Ez csak egy esetben hatékony, amikor a WEPplus-t a vezeték nélküli hálózati kapcsolat mindkét oldalán használják. Ez nehezen érvényesíthető, sorozatos korlátozást von maga után, így lehetséges a sikeres támadások indítása a WEPplus ellen is. Ez sem véd meg szükségszerűen az ismétlődő támadásoktól.

4.2.4. Dynamic WEP

A Dynamic WEP = Dinamikus WEP a WEP kulcsokat dinamikusan cseréli. Ez egy gyártó specifikus tulajdonság, amiről csak néhány gyártó gondoskodott, mint például a 3Com.

A dinamikus csere ötlete a 802.11i szabványban lett leírva a TKIP részeként, de nem az aktuális WEP algoritmushoz.

Hiányosságai

A titkosított tunelling (port továbbítási) protokollok használata gondoskodik az adatátvitel biztonságosságáról egy nem biztonságos hálózaton keresztül.

Lehetővé tesz, bizonyos belső hálózati címek külső elérését egy megadott porton keresztül. A port továbbítás rendkívül hasznos minden olyan feladat esetében, ahol egy adott lokális hálózat egyik belső IP-címét akarjuk elérni egy külső gépről. A vezeték nélküli hálózatokban azonban a WEP helyettesítésére folyamatos fejlesztésre van szükség, a szintén folyamatosan bővülő biztonsági elvárások miatt.

4.2.5. WPA

2003-ban a Wi-Fi Aliance (Wi-Fi Szövetsége) az eddigi WEP-et hatálytalanítja és helyébe az újonnan kifejlesztette a WPA-t (Wi-Fi Protected Access, magyarul Wi-Fi védett hozzáférés). A WPA tervezése során komolyan vették a biztonságot, ezért egy roppant jól kezelhető és ellenálló protokollnak tekinthető. WPA rendszer automatikusan generálja a PSK jelszót, következetes módon, minden hálózati kapcsolatnál új kulcsot alkalmaz (tehát a különböző számítógépek, hozzáférési pontjaik, és a kliens eszközeiket egyaránt). Így kiküszöböli a statikus WEP kulcs problémáját.

A WPA alapját az IEEE 802.11i szabvány képezi, amely tartalmazza főbb szabványait, 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 WPA tulajdonképpen magába foglalja a TKIP (Temporal Key Integretiy Protocol) titkosítási és a 802.1X mechanizmust. Ez a két mechanizmus biztosítja a dinamikusan kódolt kulcsokat, a kölcsönös hitelesítést, akár egy nagy erőforrás igényű vezeték nélküli hálózatnál is. A TKIP protokoll lehetővé teszi a lehetséges legfontosabb változásokat, és automatikusan szinkronizálja a hozzáférési pontot a vezeték nélküli klienssel. Egy Wi-Fi hálózat összes eszközének (hozzáférési pontjai, routerei, kliens eszközei, stb.…) szükség van egy hozzáadott

hardvergyorsítóra a titkosítás elvégzéséhez. Arról nem is beszélve, hogy a régi WEP-es berendezések, amelyek nem támogatják a WPA titkosítást nem fogják frissíteni. Nem lehet csak úgy keverni a titkosítást. Ilyenkor érdemes 2 hálózatot kiépíteni, és a legtöbb tevékenység a WPA hálózaton fut, és megtartva a régi WEP felszerelést fut egy másik csatornán (külön hozzáférési ponttal).

Akár a WEP-nél itt is az adatok titkosítása az RC4 adatfolyam titkosítóval történik, 128-bit kulcs használatával és egy 48-bites induló inicializáló vektorral. A legfontosabb fejlesztés a WPA-n belül a WEP-hez képest a TKIP (Temporal Key Integity Protocol) bevezetése, amely véletlenszerűen változtatja az alkalmazott 128 bites kulcsokat. Ezzel hidalva át a jól ismert kulcs-megszerzéses támadás-t a WEP-ben. Mindaddig megfelelő ez a titkosítás, ameddig egy felhasználó ki nem találja a WPA jelszót.

A vezeték nélküli hozzáférési pontok a WPA és WEP titkosítást egyidejűleg is támogatnak, ez a lehetőség a fokozatos átmenetet teszi lehetővé. Egyetlen egy dologra kell odafigyelni, a 2 titkosítás keverésénél, hogy a WEP ügyfelek nem támogatják az automatikus kulcs cserélést.

Csomagonkénti forgalmazása az egyik legerősebb tulajdonsága. A WPA automatikusan létrehoz egy új egyedi titkosító kulcsot bizonyos időközönként minden egyes ügyfélnek. Valójában minden egyes csomagnak ad egy egyedi kulcsot.

Kezdetben, a vezeték nélküli hálózatoknál a kliens hitelesítette a hozzáférési pontokat, amely engedélyezi, hogy az ügyfél küldhet keretet a hozzáférési ponthoz. Mára már felhasználói szintű hitelesítést készít.

A WPA még mindig biztonságos csak naprakésznek kell lennünk a frissítéseikkel.

Két változata:

- A vállalati WPA-Enterprise mód. Egy authentikációs szervert használ a működéséhez, amely azonosítja a felhasználót és gondoskodik a titkosító kulcsok rendszeres cseréjéről (rekeying). A vállalati üzemmód a nagyvállalatok és az állami szervezetek igényeit elégítik ki.

- A személyes WPA-PSK (Pre Shared Key) módban, amit valószínűleg a legtöbben választanak otthon és kishivatali környezetben. Nincs szükséghitelesítő kiszolgálóra. Ez egy kicsit „butább” változat. Mindenki egy közös PSK jelszót használ. A megadandó jelszónak hosszabbnak kell lennie, mint a jellegzetes 6-8 karakter, amit az átlagfelhasználók általában még elfogadhatónak tartanak. Ez a hitelesítő mód nem a legbombabiztosabb megoldás, de a törés gyakorlatilag csak akkor valósítható meg, ha a felhasználó gyenge jelszót választott. Már sokkal biztonságosabb volt, de csak egy átmeneti megoldásnak szánták, míg az IEEE 802.11i szabványt véglegesítették.

További erősségei WPA-nak

A hitelesítésben és titkosításban történt fejlesztéseknek köszönhetően a WPA-ban nagymértékben javult a letöltött adatcsomagok integritása. A WEP-ben lévő kevésbé 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 üzenethitelesítési 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 Inicializáló Vektorok méretének növekedésével, a jól ismert 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 illesztőivel 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.

Néhány WPA törési szoftverek Linux alatt:

- Kismet: a hálózat feltérképezésére szolgáló alkalmazás. A 802.11 2 rétegének, vezeték nélküli hálózati figyelő és behatolás észleléses-rendszere. A Kismet dolgozni fog bármilyen vezeték nélküli hálózati kártyával, amely ismeri 802.11b vagy 802.11a vagy 802.11g protokoll egyikét. A Kismet hálózatokat azonosít, ha passzív csomagokat észlel és ez által az adatforgalmon keresztül épít ki hálózatot.
- *Aireplay*: csomag elfogása és küldése a hálózatba.
- *Cowpatty*: WPA jelszó feltörése brute force módon.

A támadás menete

A hitelesített kliens leválasztása az AP-ról deautentikációs kéréssel. Az újbóli autentikációs csomagok elfogása. Az elfogott csomagokból a jelszó visszaállítása.

4.2.6. WPA2

2004-ben szinte párhuzamosan elődjével a WPA-val fejlesztették ki a WPA2-t, ez jelenleg a legbiztonságosabb technológia, feltörési lehetősége MÉG nem ismert. A WPA2 a mai generáció Wi-Fi biztonsága. Főleg az új AES (Advanced Encryption Standard) algoritmust használja, amellyel szinte teljesen biztonságossá tették.

Az IEEE 802.1X szabvány széles körben használt vállalati hálózatoknál, amiért megbízható hitelesítést biztosít és fejlett hálózati hozzáférés-ellenőrző funkcióval rendelkezik. Emellett az IEEE 802.11i szabványt használ személyes módban, amely egy 128 bites AES-alapú titkosítást alkalmaz, ezzel biztosítja a kölcsönös hitelesítést.

Minden vezeték nélküli hálózati eszköz titkosítja a hálózati forgalom segítségével a 256 bites kulcsot. Ez a kulcs lehet 64 bites hexadecimális számjegy, vagy 8-63 nyomtatható ASCII karakter (ezt 256 bites kulcs alkalmazásával kerül kiszámításra).

A WPA2 visszafelé kompatibilis a WPA-val, de a WEP-pel már nem. Hiszen a Wi-Fi Alliance nem tartja biztonságosnak, így biztonsági okokból nem támogatja.

Akárcsak a WPA-nál, a WPA2-nél is egyaránt kínál személyes (Personal) és vállalati (Enterpise) üzemmódot. Személyes üzemmódban előre megosztott kulcs használatos a hitelesítésnél, amíg a vállalati üzemmódban, a hitelesítés (EAP) útján valósul meg. A személyes mód csak a szükséges hozzáférési pont és kliens eszközöket biztosítja, ezzel ellentétben a vállalati mód megköveteli a RADIUS (Remote Authentication Dial A User Service) vagy más autentikációs szervert a hálózaton. Ez egy hálózati kliens / szerver protokoll, amely központosított azonosítást, engedélyezést és számítások kezelését szabályozza a számítógépeken a hálózathoz csatlakozás során. A RADIUS szerver hátterében futó folyamat – 3 funkciója van:

- A felhasználók vagy eszközök hitelesítése, mielőtt hozzáférést kapna a hálózathoz.
- Engedélyezi a felhasználóknak és eszközöknek azokat a hálózati szolgáltatásokat, amelyekre szükségük van.
- Figyelembe veszi ezeknek a szolgáltatásoknak a használatát.

2004-ben a Wi-Fi Alliance vezette be a WPA2 tanúsítványt. 2006-tól kötelezővé vált az összes Wi-Fi CERTIFIELD berendezések minősítésének benyújtását. Minden vezeték nélküli eszköz, kötelezően ezzel a szabvánnyal készül. Tehát ha vezeték nélküli hálózatot szeretnénk kiépíteni, akkor mindenképpen a WPA2 az ajánlatos titkosítás.

Változat	*Titkosítás*	*Hitelesítés*	*Leírás*	*Összehasonlítás*
WPA – Personal	TKIP	PSK	- Egyszerű beállítás	- Gyengébb titkosítás - Gyenge jelszavakra érzékeny
WPA – Enterprise	TKIP	RADIUS + EAP	- Robusztus hitelesítés	- Gyengébb titkosítás - Szükséges egy RADIUS szerver beszerzése
WPA2 – Personal	EAS	PSK	- Egyszerű beállítás - Erős titkosítás	- A gyenge jelszavakra érzékeny - Lehetséges, hogy nem támogatja a régebbi változatokat
WPA2 – Enterprise	AES	RADIUS + EAP	- Robusztus hitelesítés - Erős titkosítás	- Lehetséges, hogy nem támogatja a régebbi változatokat - Szükséges egy RADIUS szerver beszerzése

5. Wi-Fi támadások

Mivel a WLAN hálózatok egyre népszerűbbek az otthonainkban, egyre többen vannak kitéve a veszélyeknek, mint például a kémprogramoknak. Valamint szükségessé válik a rendszer biztonságosabbá tétele.

5.1. Brute force

A Brute force támadás (szó szerinti fordításban: nyers erő), más néven teljes kipróbálás módszere, egy, a titkosító rendszerek ellen alkalmazott támadási mód, ami meglehetősen eredményes.

Működésének lényege, hogy a titkosító rendszerek ismeretében az összes lehetséges kulcsot kipróbálva határozza meg a használt kulcsot. Eredményességét igazából csak az informatikai háttér és az idő határozza meg. Gyors és nagy kapacitású számítógépre van szükség. A törés kizárólag a kulcs méretétől és bonyolultságától függ.

$$\text{Lehetséges kulcsok száma} = (\text{karakterek száma})^{\text{kulcs hossza}}$$

A kulcsaink folyamatos cseréjével a betolakodót folyamatos kulcsrakészségre kényszerítjük.

5.2. Wardriving

Egy olyan tevékenység, melynek keretében egy adott földrajzi területen, olyan Wi-Fi hálózatok után kutatnak, amelyek nincsenek levédve, ezért oda be tudnak lépni. Sajnos ez utóbbi tevékenység kezd egyre népszerűbbé válni, pedig a wardriving eredetileg a hálózatok nevének/helyzetének felderítéséről szólt, nem pedig arról hogy a szomszédunk hálózatát használjuk. Általában a tevékenység közben autóban mozognak, de történhet gyalog vagy biciklivel is.

Az ilyen hálózatokba való belépés nem törvénytelen, de etikátlan, mert mások berendezését és a mások által fizetett sávszélességet használja, és személyiségi jogi kérdéseket is felvet, hiszen ez által a wardriver mások személyes adataihoz fér hozzá. Már törvény tiltja más Wi-Fi hálózatát használni.

A Wardriving egy vitatható gyakorlat, de segített felhívni a figyelmet a fontosságra és a WLAN-ok biztonságára.

5.3. Warspamming

Ennek a támadásnak az a célja, hogy korlátozás nélkül küldjön reklám leveleket. A hackerek élvezhették a bizonytalan Wi-Fi hálózatok előnyét, hogy terjessze reklámjaikat. Segítségre volt, hogy győzedelmeskedjenek a spam listakezelő programok ellen (pl. Spamhaus) kijátszása. Ha sikerült hozzáférési pontot találni, akkor kinyomozhatatlan a küldő kiléte.

5.4. Evil twin

A hackerek egy Wi-Fi hálózat hozzáférési pontját kihasználva épít ki hálózatot közöttünk. A lényeg, hogy interneten való szörföléseink között hallgasson le kommunikációt.

A hacker a számítógépet úgy konfigurálhatják, hogy a törvénytelen hozzáférési pontra irányítja, ahol felügyelni tudja az áldozat forgalmát. Könnyedén elcsenhetik személyes adatainkat és jelszavainkat. Vegyük például azt a példát, hogy egy kávézóban használunk vezeték nélküli hálózatot, ahol kapcsolódási díjat kell fizetni. Kapcsolódásnál, meg kell adni a bankkártya számát és bizonyos személyes adatokat. Egy tipikus evil twin csalás, hogy valaki egy saját hálózati pontját, amely hamis hálózati nevet tartalmaz felváltja a regisztrációs lapot a hasonmásával. Mindezek után a hacker nem a hot spot szolgáltatónak adja át az adatait, hanem átirányítja más hot spotoknak.

5.5. Lehallgatás

Cél, hogy a szerver és/vagy kliens azonosított legyen. Egy szerver hitelesítését egy külső intézmény, a tanúsítványt kiállító szervezet végzi.

Ez olyan esetben szükséges, ha fontos a látogatóknak, hogy a szervertől meg tudják állapítani, hogy tényleg az övék e. Bankoknál ez elengedhetetlen, egyéb esetekben ritka, hogy erre szükség lenne. A két funkció és annak tényleges megvalósítása nagyon fontos!

5.6. Adattitkosítás

Célja, hogy garantált legyen, hogy a kiszolgáló és a böngésző közötti kommunikáció titkosítva történjen, így az ne legyen lehallgatható vagy módosítható.

A https kommunikáció egy védett csatornán zajlik, nem nyújt védelmet, ha a végpontokon történik a “lehallgatás”, tehát például a kliens gépen egy nem kívánt program fut!

Erre ritkán van szükség, leginkább olyan esetben, ha bizalmas adatokat kezelnek egy ügyfélnek (például online fizetés esetén a bankkártya számok). Viszont ritkán olvasni arról, hogy visszaélés történne egy közbenső ponton, inkább egy munkaállomásra települt kémprogramnál jelent veszélyt.

6. 10 tipp otthoni vezeték nélküli hálózatunk beállítására

Sok ember létrehoz, egy vezeték nélküli otthoni hálózatot a lehető leggyorsabban, hogy Internet-kapcsolat működjön, aztán rohan a munkahelyére vagy éppen a gyerekekért. Ez teljesen érthető, de elég kockázatos is, számos biztonsági problémát okozhat. Az általános felhasználó nincs is tisztában mekkora kockázattal jár, a nem megfelelően beállított hálózat. A mai Wi-Fi hálózati termékek nem mindig segítik a hálózat konfigurálásának biztonsági

lépéseit, általában az alapértelmezett beállítás a leggyengébb. Egy hálózatot optimálisan beállítani időigényes. Az ajánlásom az alábbiakban foglalja össze a lépéseket, amelyeket nem árt megtenni, hogy javítsa a biztonságot az otthoni vezeték nélküli hálózatunkon.

Ezek közül több tipp is valószínűleg nem alkalmazható számos hálózatnál. Például, ha fut a vezeték nélküli hálózat, amely lehetővé teszi a kapcsolatot változó felállásban is, így az adott számítógép a hálózat nem lesz állandó, az a pont korlátozza a hozzáférést a MAC-címekhez. Mindenki próbálja meghatározni a biztonsági tippek közül azokat, amelyek önökre vonatkozhatnak.

Megpróbálom szemléltetni is egy DIR-600 - Wireless N 150 Routerrel.

1. Használjon erős jelszót.

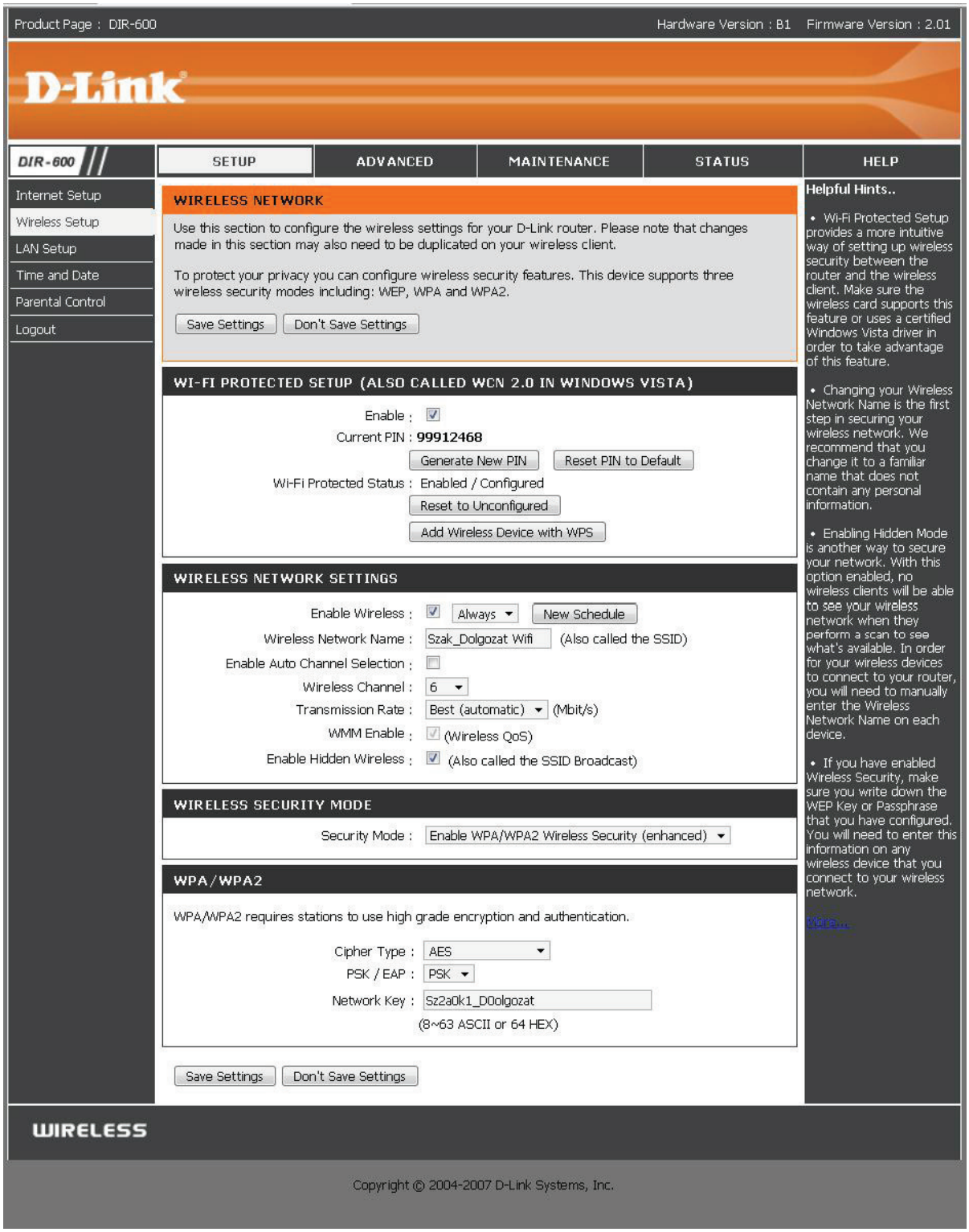
Változtassa meg az alapértelmezett jelszót – az alapértelmezett jelszavak nem biztosítanak szilárd biztonságot. Meg lehet változtatni mind a hozzáférési pont vagy útvonalválasztó jelszavát is.

A kellően erős jelszó lehetővé teszi, hogy a brute force támadásokat gyakorlatilag lehetetlenné tesszük a crackarek számára. A kellően gyenge jelszavak használata, szinte garantálja, hogy a rendszer veszélybe kerüljön.

2. Használjon jó vezeték nélküli titkosítást.

Az összes Wi-Fi berendezés támogatja valamilyen formában a titkosítást. A titkosítási technológiák összekuszálják a küldött üzeneteket a vezeték nélküli hálózaton, hogy ne lehessen olyan könnyen kiolvasni. Számos titkosítási technológia létezik, fentiekben már említettem őket. Érdemes a legerősebb formáját alkalmazni.

A WEP nem éppen a legmegfelelőbb titkosítás. Használjunk WPA vagy WPA2 titkosítást, mára már ez a közös titkosítási szabvány a legelterjedtebb. Bár a technológiai fejlődések a mindennapjainkban, a titkosító fegyverkezési versenyben, nincs tökéletes védelem.



3. <u>Módosítsuk az alapértelmezett SSID-t.</u>

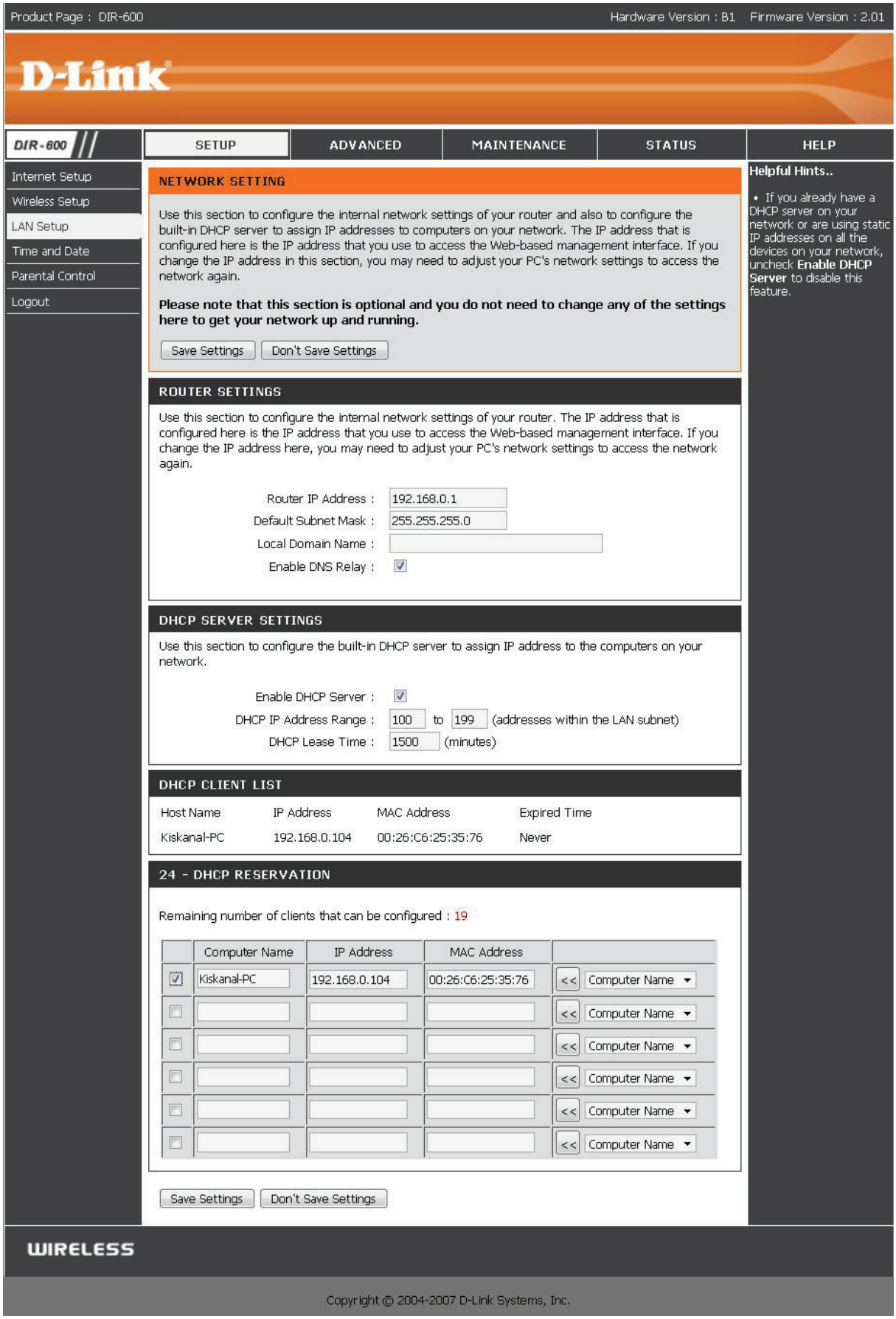
Hozzáférési pontok és útvonalválasztók mindannyiik a hálózat nevét az úgynevezett SSID-t használják. A gyártók általában ugyanazt az SSID-t adják meg. Például a Linksys eszközöknél

általában a „linksys”. Ismerve az SSID-t önmagában még nem teszi, lehetővé a szomszédok behatolását a hálózatunkba – de ez csak a kezdet. Ennél sokkal fontosabb, ha valaki talál egy alapértelmezett SSID-t, akkor látják a rosszul konfigurált hálózatot és sokkal, nagyobb valószínűséggel fogják támadni.

4. Korlátozza a MAC-cím hozzáférését.

Ne higgyük, hogy a titkosításunk minden biztonságot biztosít a hálózatunknak.

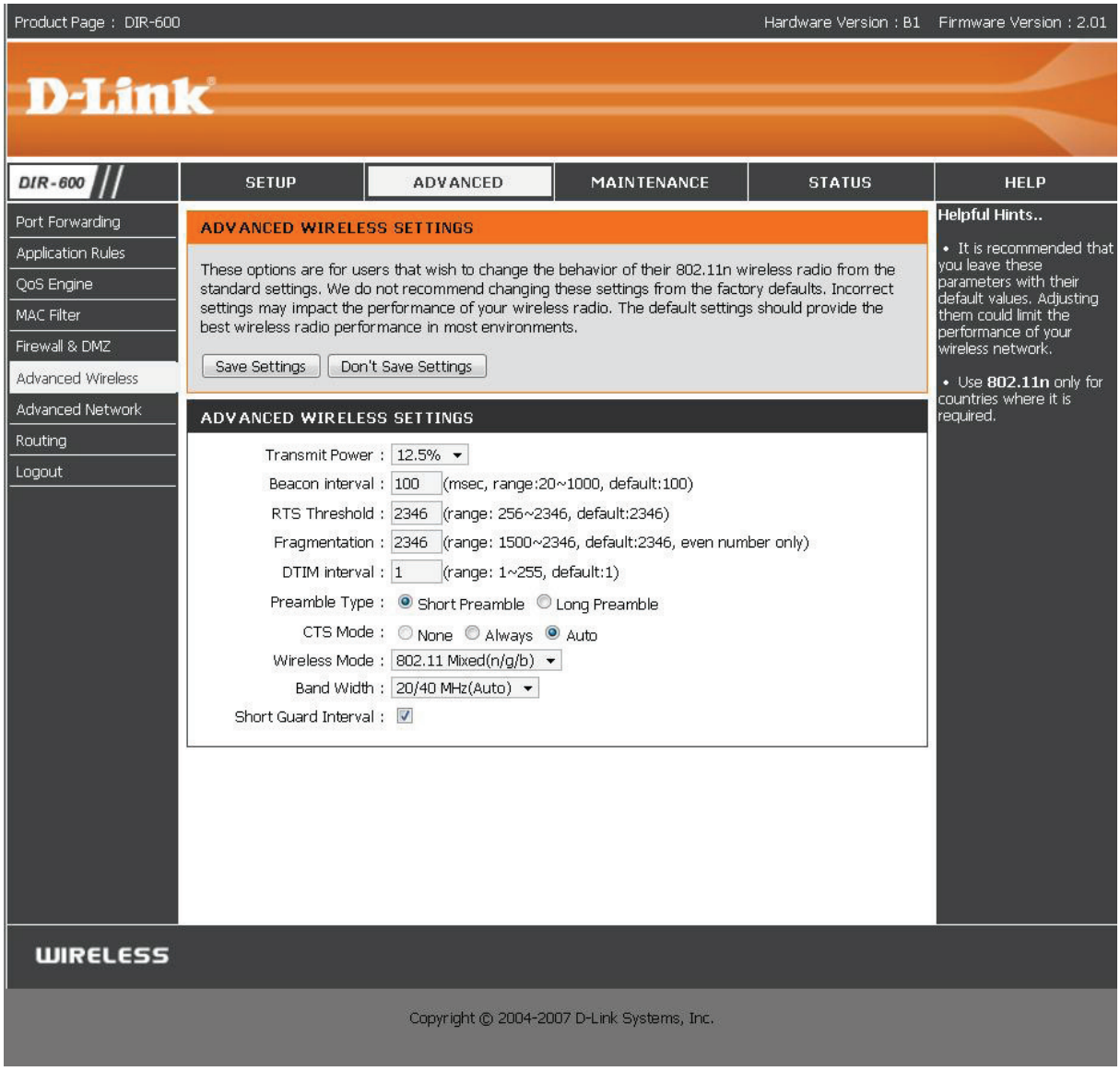
Minden egyes Wi-Fi-s eszköz rendelkezik egy egyedi azonosítóval az úgynevezett fizikai címmel vagy más néven MAC címmel. A hozzáférési pontokat az útvonalválasztók nyomon követik az összes MAC címet, hiszen az összes eszköz hozzájuk csatlakozik. Számos ilyen terméket kínálnak a gyártók, ahol a tulajdonosnak van lehetőse megadni a MAC címet a saját berendezéseiről, így csak akkor engedélyezi a kapcsolatot, ha a korlátozásba még belefér az eszköz.


Product Page : DIR-600
Hardware Version : B1
Firmware Version : 2.01
D-Link
DIR-600
SETUP
ADVANCED
MAINTENANCE
STATUS
HELP
Internet Setup
Wireless Setup
LAN Setup
Time and Date
Parental Control
Logout
NETWORK SETTING
Use this section to configure the internal network settings of your router and also to configure the built-in DHCP server to assign IP addresses to computers on your network. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address in this section, you may need to adjust your PC's network settings to access the network again.
Please note that this section is optional and you do not need to change any of the settings here to get your network up and running.
Save Settings
Don't Save Settings
ROUTER SETTINGS
Use this section to configure the internal network settings of your router. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again.
Router IP Address : 192.168.0.1
Default Subnet Mask : 255.255.255.0
Local Domain Name :
Enable DNS Relay :
DHCP SERVER SETTINGS
Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.
Enable DHCP Server :
DHCP IP Address Range : 100 to 199 (addresses within the LAN subnet)
DHCP Lease Time : 1500 (minutes)
DHCP CLIENT LIST
Host Name
IP Address
MAC Address
Expired Time
Kiskanal-PC
192.168.0.104
00:26:C6:25:35:76
Never
24 - DHCP RESERVATION
Remaining number of clients that can be configured : 19
Computer Name
IP Address
MAC Address
Kiskanal-PC
192.168.0.104
00:26:C6:25:35:76
<<
Computer Name
Save Settings
Don't Save Settings
Helpful Hints..
• If you already have a DHCP server on your network or are using static IP addresses on all the devices on your network, uncheck Enable DHCP Server to disable this feature.
WIRELESS
Copyright © 2004-2007 D-Link Systems, Inc.

5. Ne sugározzon SSID-t.

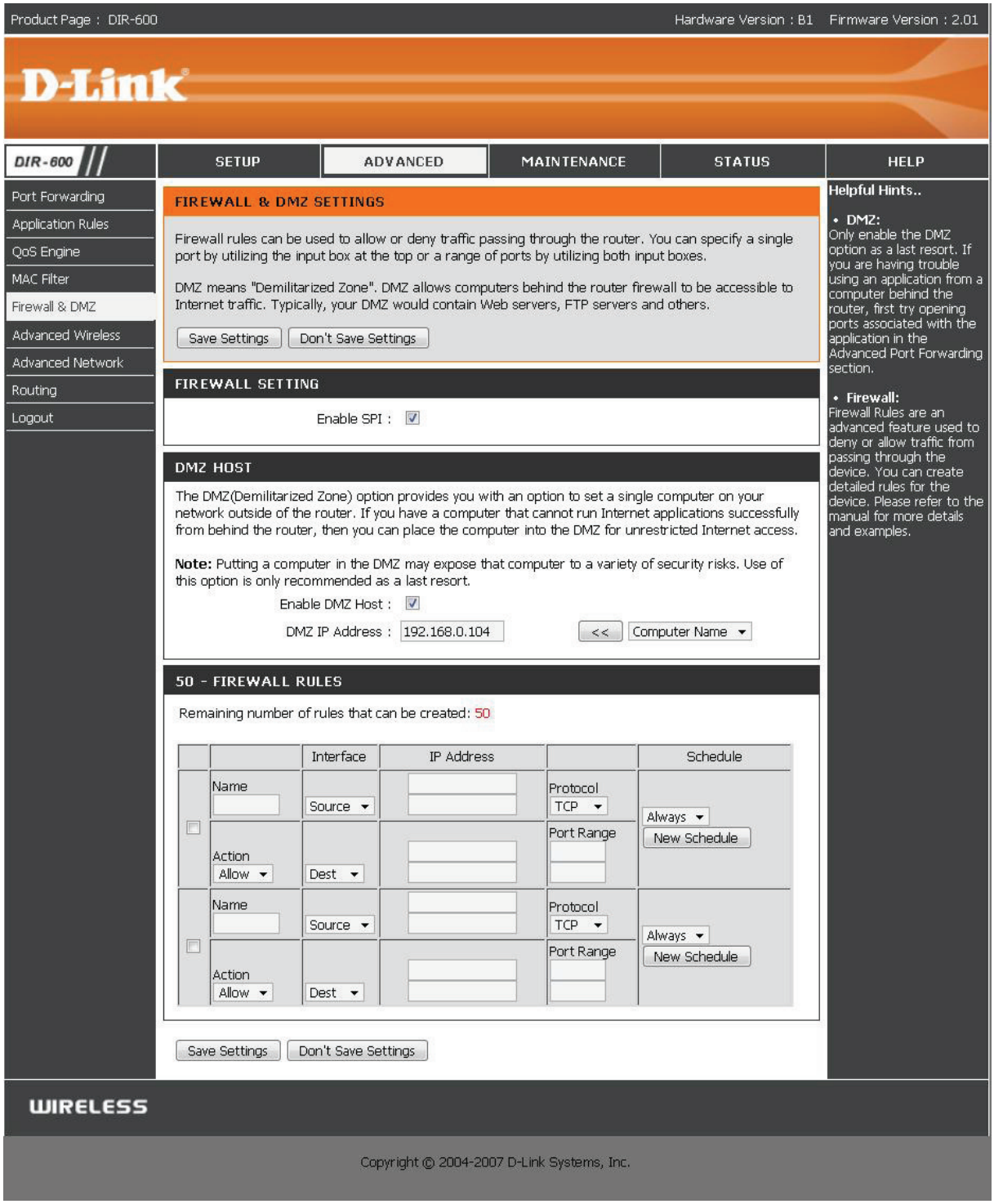
A Wi-Fi hálózatok, a vezeték nélküli hozzáférési pontok vagy útválasztók általában sugározzák a hálózati nevet (SSID) a levegőben – rendszeres időközönként. Ennek a funkciónak volt a célja a vállalkozások és a mobil hot spotok, ahol a Wi-Fi ügyfelek vándorolnak ki a tartományból. Az otthoni hálózatban ez felesleges, hiszen csak annak a kockázatát növelnénk, hogy valaki megpróbál belépni az otthoni hálózatunkba, mivel az SSID önmagában nem titkosít. Szerencsére a legtöbb Wi-Fi hozzáférési pont lehetővé teszi az SSID broadcast cím letiltását a rendszergazda által.

Ne feledjük, hogy a letiltott SSID broadcat csak egy a sok szigorító módszer közül. Ez a technológia sem 100%osan hatékony. De alkalmazásával megbénít néhány betolakodót, hiszen valószínűleg egyszerűbb feladatot találnak 2 lakással távolabb.



6. <u>Tűzfal és frissítések engedélyezése minden számítógépen és routeren.</u>

Fontos felszerelkezni további biztonsági mechanizmusokkal, mint például tűzfal és vírusirtó programok. Hiszen a rosszindulatú hackerek és rosszindulatú szoftverek fejlődnek a napi rendszerességgel fontos hogy ezeket a programokat folyamatosan a legújabb frissítéseket megkapják a gyártói adatbázisból. Győződjön meg arról, hogy valami jó tűzfal fut az operációs rendszerünkön. Ezen felül a modern hálózati routerek is tartalmaznak beépített tűzfalat, de a lehetőség is fennáll, hogy letiltsuk azokat. Ellenőrizzük, hogy a router tűzfala be van e kapcsolva, ha véletlenül, nincs, akkor tegyük meg azt.



7. <u>Ne engedélyezd az automatikus csatlakozást nyílt Wi-Fi hálózatokhoz.</u>

Kapcsolódás a nyílt Wi-Fi hálózathoz, például ingyenes vezeték nélküli hot spot, vagy a szomszéd router teszi ki a számítógépet, a biztonsági kockázatokra. Bár általában nem engedélyezett, amely lehetővé teszik, hogy ezek a kapcsolatok automatikusan történnek

anélkül, hogy erről még akárcsak a felhasználó is tudna. Ez a beállítás nem engedélyezett, kivéve ha lehetséges az átmeneti helyzet.

8. Figyelemmel kísérni a hálózatunk „betolakodóit”.

Mindig győződjünk meg arról, hogy mi folyik éppen a hálózaton. Rengeteg eszköz vagy alkalmazás létezik már, amely figyeli a rendszer tevékenységét, és jelentéseket készít a számítógépes rendszerről vagy hálózatról. Ezeket a jeleket elemzi, hogy lehetséges esemény következtében történt, vagy olyanok, amelyekkel megsértik a biztonsági politikát. A behatolás észlelési és védelmi rendszerek elsősorban összehangol olyan lehetséges eseményeket, amelyek megpróbálják megállítani a behatolókat.

9. Az útválasztót vagy a hozzáférési pontot biztonságosan helyezzük el.

Wi-Fi-s jelek általában elérik az otthon külső falait. A silány jelek szivárgása a szabadban nem probléma, de ha mások elérik ezt a jelet, annál könnyebb a mások számára a felderítés és a kiaknázás. A jeleink gyakran elérik a szomszédos házakat és akár az utcát is. Amikor telepítünk egy vezeték nélküli otthoni hálózatot a hozzáférési pont vagy útválasztó határozza meg az elérési út hosszát. Próbáljuk ezeket az eszközöket a lakás közepébe helyezni és minél kevesebb ablak köré – ezzel is csökkentsük a szivárgás kockázatát.

10. Állítsuk le a hálózatunkat, ha hosszú távon nem használjuk.

A végső vezeték nélküli biztonsági intézkedések, hogy leállításuk a hálózatunkat. Minden bizonnyal megakadályozzák a külső hackerek betörését, ha megszüntetjük a kapcsolatot. Másrészről nem célszerű gyakran ki és bekapcsolni a készülékeket.

Ha van egy mobil eszközünk, mint például egy notebook, amit hordozunk és használjuk nyilvánosan, akkor alapértelmezetten ajánlott kikapcsolni a hálózati belépési pontunkat, és csak abban az esetben bekapcsolni, ha valóban csatlakozni kívánunk a hálózathoz. Ha nem így járunk el – újabb támadási felületet és időt hagyunk a rosszindulatú crackereknek.

Ezek az egyszerű ötletek segíthetnek biztonságosabbá tenni a számítógépeinket és hálózatunkat.

7. Köszönetnyilvánítás

Szeretném megköszönni Dr. Krausz Tamás témavezetőmnek a szakdolgozatom elkészítéséhez adott segítő tanácsait, javaslatait és a segédanyagok rendelkezésemre bocsájtását.

8. Összegzés

A vezeték nélküli hálózatok korábbi biztonságtechnikai problémái megoldódni látszanak az IEEE 802.11i és IEEE 802.11y szabvány bevezetésével. Mivel ezek a technológiák elég újak, a bevezetésük folyamatosan történik. A WLAN hálózatok biztonsági problémái miatt sajnos sok biztonsági követelménynek megfelelő rendszerben ez idáig nem szívesen alkalmazták. A WPA és WPA2 titkosítási eljárással biztonságos hátteret biztosít a vezeték nélküli hálózatoknál, ezért az ez idáig tartózkodók is nyugodt szívvel alkalmazzák.

Az autentikációs és adattitkosítási problémák megoldásával, illetve a sebesség további növelésével remélhetőleg egyre többen bíznak majd a vezeték nélküli technológiákban és az elterjedése folyamatosan nőni fog.

Szakdolgozatom kidolgozása során megpróbáltam amennyire lehet részletesen megismertetni a WLAN technológiákat, biztonsági oldalról. Bemutattam legújabb vezeték nélküli biztonsági megoldásokat. Természetesen ez sosem lesz elég, hiszen az informatika területén 100%-os biztonság azonban nem létezik. A felhasználók egyre jobban követelik a biztonságot, azonban tudatosítani kell bennük, hogy a hálózat megbízhatóságához ők is hozzájárulnak az adatok bizalmas és felelősségteljes kezelésével. Végül bízom benne, hogy az általam bemutatott legújabb szabványokkal és újszerű módszerekkel hozzájárultam az otthoni hálózattervezők eredményes munkájához.

9. Irodalomjegyzék

[Buttyán Levente és Dóra László]:
WiFi biztonság – A jó, a rossz, és a csúf

[Krasznay Csaba]:
Vezeték nélküli hálózatok biztonsága

[Danny Briere and Pat Hurley]:
Wireless Network Hacks & Mods For Dummies

[Chris Hurley, Russ Rogers, Frank Thornton, Daniel Connelly, Brian Baker]:
WarDriving & Wireless - Penetration Testing

[Lee Barken]:
Wireless Hacking: Projects for Wi-Fi Enthusiasts

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

[Dr. Pethő Attila]:
Az informatikai biztonság alapjai

[McGraw.Hill]:
CWNA Certified Wireless Network Administrator Official Study.Guide

http://aboba.drizzlehosting.com/IEEE/rc4_ksaproc.pdf

http://alpha.tmit.bme.hu/meresek/wlan.htm#wlanprocon

http://blogs.techrepublic.com.com/security/?p=364

http://compnetworking.about.com/

http://compnetworking.about.com/od/networksecurityprivacy/l/aa011303a.htm

http://ecommerce.hostip.info/

http://hadmernok.hu/archivum/2007/2/2007_2_takacs.html

http://howto.techworld.com/security

http://hu.opensuse.org/Dokument%C3%A1ci%C3%B3/SL9.3/Rendszer/Vezet%C3%A9kn%C3%A9lk%C3%BCli_kommunik%C3%A1ci%C3%B3

http://hu.wikipedia.org/wiki/Wifi

http://krono.inaplo.hu/index.php/inter/8-networkstudies/850--wifi

http://mycite.omikk.bme.hu/doc/41352.pdf

http://pajhome.org.uk/crypt/rsa/rsa.html

http://phserver.phy.georgiasouthern.edu/rldeal/m685/wnic/Docs/HUN/security.htm

http://techrepublic.com.com/

http://uninformed.org/

http://www.bcs.hu/hu/tudastar/wireless_tudastar/

http://www.microsoft.com

http://www.mycrypto.net/encryption/public_key_encryption.html

http://www.networkworld.com/

http://www.offensive-security.com/resources/

http://www.patownsend.com/cms_uploads/file/WhitePapers/AES_Introduction.pdf

http://www.smallnetbuilder.com/

http://www.spamlaws.com/

http://www.technet.hu/hir/20051229/vezetek_nelkuli_halozat_otthon_-_iii_resz/

http://www.technet.hu/pdamania/20051014/vezetek_nelkuli_halozat_otthon_-_i_resz/

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

http://www.wi-fiplanet.com/tutorials/

http://www.wirelessdevnet.com/

http://www.wyonair.com/

www.google.com