Debreceni Egyetem
Informatika kar

Vezeték nélküli hálózatok biztonsági kérdései

Témavezető:
Dr. Krausz Tamás
Egyetemi adjunktus

Készítette:
Borics Ákos
Programtervező Informatikus

Debrecen
2009

Bevezető

A számítástechnika mára, az átlag ember életének is nélkülözhetetlen részévé vált. A családok többségében, ki munkájából kifolyólag, ki tanulmányaihoz kapcsolódóan, ki pedig csak egyszerű tudásvágyból vagy kikapcsolódásból használja a számítógépek különböző konfigurációjának valamelyikét. Ennyi igényt egy időben egyetlen számítógép, nem tud kielégíteni, ezért sokszor előfordul, hogy több számítógép is van egy azon háztartásban. Ahol több felhasználó és számítógép van, ott pedig előbb-utóbb felmerül az adatcsere vagy az erőforrásmegosztás, ill. az egymással kommunikálás kihasználásának gondolata. Ez a gondolat pedig előteremti a hálózat megteremtésére való igényeket.

A hálózatok kialakítására számos megoldás létezik, ilyenkor figyelembe kell venni a lehetőségek előnyeit, hátrányait, illetve a hálózattal szemben támasztott igényeket. A számítógépek hálózatba szervezése lehetséges kábellel való összekötéssel, és vezeték nélküli összeköttetéssel. A vezeték nélküli hálózatok megteremtésében vannak különböző szabványok, manapság a legelterjedtebbek a 802.11b, 802.11g,802.11a. Az imént felsorolt szabványok frekvenciatartományukban, modulációjukban és ebből a két tulajdonságból adódóan sávszélességükben térnek el egymástól. Ma már a számítógépek nem csak otthoni, vagy lokális hálózatba vannak kötve egymással, de a legtöbb a világhálóhoz is csatlakozik (Internet). Ennek következtében az adataink bizony komoly veszélyeknek vannak kitéve még a vezetékes hálózatok esetén is. Az internet segítségével ugyanis, akárki akármilyen messze is jogosulatlanul hozzáférhet adatainkhoz. A hétköznapi ügyek intézését is egyre több ember intézi távoli kapcsolattal, vagy interneten. Az ilyen ügyek intézése közben is, mint például egy banki tranzakció, vagy vásárlás, kitudódhatnak olyan információk, amik nem csak, hogy kényesen érinthetik a személyeket, hanem még súlyos anyagi károkat is okozhatnak.

Biztonságunk érdekében, lehetőségeinkhez mérten, ki kell zárni annak esélyét, hogy illetéktelenek ne tudják gépünket használni. A kábeles kapcsolat esetén, minden lehetséges támadásnak szemmel látható nyomai vannak, mégis nagyon nehéz ellenük védekezni. A vezetéknélküli hálózatok esetében azonban nem elég, hogy nem marad látható nyoma, hanem még ha a jelerősség elég erős akkor a jogosulatlan hozzáférő távolabbról is tud csatlakozni, és már csak a hitelesítés, illetve a különböző kódolások,titkosítási protokollok

állnak az útjába . A fizikai csatlakozás után, már csak a különböző jelszavak,azonosítók és hitelesítések hiányoznak az adatokhoz való hozzáférés előtt, ezek teljesülését szoftveres és hardveres mechanizmusokkal lehet védeni. Azonban ezek nem az illetéktelen hozzáférések ellen készültek, hanem a hálózaton levő adatok védelme érdekében, tehát mint leírtam a vezetékes hálózatok fizikai hozzáférésének elérése után nincs más korlátozás. A vezeték nélküli hálózatok esetében viszont a fizikai hozzáférésen kívül, a biztonsági szinttől függően több, különböző adattitkosítással is számolnia kell a támadónak.

A továbbiakban és a tárgyalás részben, mint a választott cím is mutatja, a wireless hálózatok biztonsági kérdéseiről, védelmi mechanizmusairól, fajtáiról, csoportjairól és tulajdonságairól lesz szó. Ez a dolgozat persze nem fogja össze az összes aprólékosan, szaknyelven leírt cikkek és könyvek tartalmát, már csak terjedelméből adódóan sem, de a némi számítástechnikai előélettel rendelkezők számára, egy átfogó képet ad arról, hogyan is lehetne biztonságosabbá tenni a vezeték nélküli „világot”.

A vezeték nélküli hálózat, fogalma és rövid ismertetése

A vezeték nélküli hálózatok is számítástechnikai eszközök között biztosít információcserét, ugyanúgy, mint az optikai, fényvezető szálas, vagy a rézvezetékes hálózat. Legtöbb esetben csak adatokat, üzeneteket, fájlokat továbbít, de a teljesítmények növekedésével nagyobb állományok, videók, hanganyagok továbbítását is lehetővé teszi.

Az ilyen hálózatok lehetővé teszik az emberek számára, hogy különböző épületrészekben, épületekben, a világ akár bármely pontján hozzáférjenek alkalmazásokhoz, információkhoz. Ez mozgásteret biztosít, például az ember a szép tavaszi napsütésben, nem kell, hogy íróasztalánál ülve írja szakdolgozatát, hanem nyugodtan kimehet a kertbe és a madárcsicsergéssel és virágillattal teli levegőn, végezheti munkáját.

A wireless hálózatok csoportosítása

A vezeték nélküli hálózatok egyik csoportosítása, az, mely az általuk lefedett fizikai terület mérete alapján osztja szét őket, e szempont szerint a következő csoportok léteznek:

- Vezeték nélküli személyi hálózat (PAN)
- Vezeték nélküli lokális hálózat (LAN)
- Vezeték nélküli nagyvárosi hálózat (MAN)
- Vezeték nélküli nagy kiterjedésű hálózat (WAN)

Az imént felsorolt típusú hálózatok már léteztek évek óta, csak vezetékes kivitelben. Ilyenek a LAN, és a WAN alapvető változatainak egyszerű kiterjesztései.

Tárgyalás

Vezeték nélküli személyi hálózatok

Ezek a hálózatok viszonylag kis hatótávolsággal rendelkeznek, ami körülbelül 15 méter, így legjobban, az ember mozgásterében és kisebb méretű helységekben működnek. A teljesítményük eléggé mérsékelt, legfeljebb 2 Mb/s. Főként a szűk környezetben lévő számítástechnikai eszközök, összeköttetését teszi lehetővé. Rendkívül kis energiafogyasztással rendelkeznek, ezért erőszeretettel használják őket mobilokban, headsetekben, és a kéziszámítógépek többségében. A vezeték nélküli hálózatok többsége az információ levegőben történő továbbítására rádióhullámot használ. Itt kell megemlíteni a Bluetooth-szabványt mely 2,4 GHz-es frekvenciasávban , 2 Mb/s adatátviteli sebességet biztosít, 15 méteres körzetben. Azonban nem csak rádióhullám segítségével történhet a kommunikáció, van olyan személyi hálózat, amely infravörös fényt használ a közvetítésre. Ezzel a módszerrel, amelyet az Infrared Data Assocation-Infravörös Adattársaság specifikációja ír le, 1 méter távolságon belül, akár 4 Mb/s adatátviteli sebesség érhető el. Az IrDA előnye, hogy nem zavarják rádiófrekvenciás jelek, hátránya viszont, hogy csak egyenes vonalban és kis távolságon belül használható, így nem is igazán használják komolyabb, illetve irodai célokra.

Vezeték nélküli lokális hálózatok

A vezeték nélküli lokális hálózatok gyárak, nagyobb épületek, lakások környezetében biztosítanak nagy adatátviteli sebességet. Ezen épületeknél, a felhasználóknak olyan laptopjai, PDA-i, eszközei vannak, melyek fejlett processzorral, használhatóan nagy képernyővel

rendelkeznek. A vezeték nélküli hálózatok ilyen fajtája hatékonyan elégíti ki az ilyen számítástechnikai eszközök összekapcsolását és az ilyen eszközökkel rendelkező tulajdonosok elvárásait. Ezt a típust a cégek nagy szeretettel alkalmazzák, mivel így biztosítanak a laptopoknak mobilhozzáférést az alkalmazásokhoz. Így aki például a konferenciateremből, vagy más helyről szeretne a vállalat, alkalmazásihoz, adatihoz hozzáférni, az, az irodájától távol is megteheti. Az alkalmazottak munkája, ezáltal sokkal hatékonyabbá tehető, ugyanakkor nagyobb szabadságérzetet, mozgásteret is biztosít számukra. Maximum 54 Mb/s adatátviteli sebessége miatt nem okoz gondot számára a nagyobb alkalmazások futtatása, vagy akár egy videó fájl lejátszása esetleg egy webkonferencia lebonyolítása. Mindezek mellett az összetevői, költségei és üzemeltetése is hasonló a vezetékes Ethernet-hálózatéhoz. Ezek a lokális vezeték nélküli hálózatok megfelelnek bármilyen otthoni, vagy vállalati környezetbe. Manapság már minden laptopba és hordozható számítógépbe telepítenek vezeték nélküli lokális hálózati adaptereket, így a legtöbb szolgáltató igénybe veszi ezeket a hálózatokat. A felhasználók bizonyos hot spotokon, vagy a nyilvános vezeték nélküli lokális hálózatok hatókörén belül, bizonyos fizetség ellenében, vagy néhány helyen már ingyen is internetezhetnek és intézhetik üzleti ügyeiket. Ilyenek lehetnek például, repülőtereken, vasútállomásokon, egyetemeken, kávézókban egyszóval olyan helyeken ahol sok ember fordul meg. A vezeték nélküli lokális hálózatoknál a legfőbb szabvány a IEEE 802.11 2.4 GHz-es és 5 GHz-es változata, melynek egy óriási hátránya hogy nem működik együtt a szabvány más változataival. Nem kapcsolható össze például a 802.11a a 802.11.b szabvány szerint implementáltakkal, mindemellett nem kevésbé fontos megemlíteni hogy biztonságilag erősen korlátozott. Ezt kiküszöbölve a Wi-Fi szövetség, az addigi szabvány bizonyos funkcióit egy úgynevezett (Wi-Fi) vezeték nélküli megbízhatóság szabványba ültette át. Ha egy termék megfelel ennek a szabványnak, akkor garantáltan együtt tud működni más termékekkel. Így a nyilvános vezeték nélküli lokális hálózatokban együtt tud dolgozni más felhasználókkal.

Vezeték nélküli nagyvárosi hálózatok

A fent említett hálózatok nagy területeket, városrészeket, településeket, egész városokat fednek le. Létezik belőle megoldás ami megoldja a mozgathatóság problémáját, de inkább az a jellemzőbb, hogy helyhez kötötten, fix módon kapcsolódnak egymáshoz. Ilyen vezeték

nélküli nagyvárosi hálózatokat hoznak létre, például a kórházak melyeknek, különböző klinikái között kell adatokat továbbítania. Szintén ezt a megoldást választják az egyetemek, főiskolák épületcsoportjai közt való adatátvitel megoldására. Vannak olyanok is, akik megrendeléseket gyűjtenek be segítségével a város más-más pontjairól. Így válik alkalmazhatóvá a vezeték nélküli nagyvárosi hálózat a már meglévő infrastruktúrák összekapcsolására, és teszi lehetővé a mobilfelhasználók számára a kommunikálást. Alkalmazását főképp, olyan helyeken használják, ahol a vezetékes vonalak kiépítése nem megoldható, ezt a problémát sok minden okozhatja, de legtöbbször a használandó területek tulajdonosaival akadnak gondok. Ahhoz ugyanis hogy a földjükön keresztül menjen a kábel, az engedélyükre van szükség, azt pedig sokszor magas ár ellenében adják meg. Adatátviteli sebessége változó, mert a két épület közt használt infravörös fény 100 Gb/s sebességet is elérheti, ugyanakkor a 30 km-es rádióhullámú összeköttetés esetén ez a sebesség maximum 100 Kb/s lehet, tehát a sebesség relatív és teljes mértékben a felhasznált eszközöktől függ. A vezeték nélküli nagyvárosi hálózat megvalósításának sok egyedi megoldása létezik, de egyre több az a hálózat, ami a már meglevő szabványokat létesíti előnyben. Egyesek annak ellenére, hogy a 802.11 szabvány az épületek belsejében használva optimális, mégis ezt a szabványt használják nagyvárosi távolságokra, olyan antennák felhasználásával, melyek a jelek egyirányú adására vagy vételére képesek. Egyre többen alkalmazzák viszont a 802.16 szabvány szerinti rendszereket, melyek nem régen kerültek ki a piacra. Ez a szabvány olyan vezeték nélküli nagyvárosi hálózatokat specifikál, melyek bizonyos távolságokon belül képesek Mb/s adatátviteli sebesség biztosítására, ezért válik egyre inkább elfogadottá az említett hálózatok körében.

Vezeték nélküli nagy kiterjedésű hálózatok

A vezeték nélküli nagy kiterjedésű hálózatok, nagy területeket, megyéket, országokat, földrészeket összekötő, mobilalkalmazásokat tesznek lehetővé. A nagy szolgáltatók erőszeretettel használják az efféle hálózatokat, hogy a rengeteg felhasználó számára nagy távolságú összeköttetést biztosítsanak. Igazából, ezek a hálózatok gazdaságosak, mert hiába a nagy távolság, és a komoly eszközök a rengeteg felhasználó miatt a költségek megoszlanak, így mind a telepítési, mind az előfizetői költségek alacsonyak maradnak. A vezeték nélküli nagy kiterjedésű hálózatok világméretű lefedettséget biztosítanak több jelentős távközlési cég

összefogása révén. Az embernek elég csak egyik szolgáltatóval szerződésben állni, és az alapján már a világ bármely pontjáról korlátozott internet szolgáltatást vehet igénybe, mert a már említett cégek roaming-egyezményeket kötöttek, melynek köszönhetően összeköttetést biztosítanak. Ezeknek a hálózatoknak igen kicsi az adatátviteli sebessége, általában csak 56 Kb/s, de azért létezik egy két 170 Kb/s közeli értékkel rendelkező is. Sávszélessége azért még kihasználható, mert léteznek információk letöltésére kialakított portálok, melyek hatékonyan tudnak együtt működni, a kis teljesítményű vezeték nélküli nagy kiterjedésű hálózatokkal. Felhasználónként viszonylag kicsi adatátviteli sebesség jut, de mivel ezt a hálózatot főképp a mobilok és a kézi számítógépek használják, így ez elfogadható. A mobiltelefonok kis méretű képernyője és a korlátozott adatfeldolgozási teljesítménye nem igényli a nagy adatátviteli teljesítményt. A vezeték nélküli nagy kiterjedésű hálózatokat használók számára folyamatosan elérhetők a hálózati alkalmazások, akárhol vannak is az irodájuktól és az otthonuktól távol, lehet az, taxi, vagy a tópart, hozzáférnek e-mailjeikhez, vállalati alkalmazásaikhoz. Az eddig felsorolt hálózatok közül ez ér el a legtöbb helyre, ezáltal biztosítva felhasználói számára az adatátvitel lehetőségét. Ennél a hálózatnál számos szabvány létezik, és mindig versenyben állnak egymással, így igen lassan fejlődnek. Az egyik legelterjedtebb volt a CDPD cellurális datagramm szolgálat, ebben az adatok 19,2 Kb/s sebességgel cserélődtek. Ez a szabvány azonban már nagyon elavult, minden valamire való szolgáltató inkább a 3G felé fordul, ami már Mb/s nagyságú adatátviteli sebesség elérésére képes. A vezeték nélküli nagy kiterjedésű hálózatok nagy hátránya, hogy kültéri használatra tervezték őket, így nem teszi lehetővé az épületen belüli lefedettségét, tehát az épület falain belül a rádiójel jelentősen gyengül.

A vezeték nélküli hálózatok előnyei

Az emberek a világ minden pontján megtekinthetik e-mailjeiket, internetezhetnek és vállalati alkalmazásokhoz férhetnek hozzá. Mivel nem kell hozzá vezeték, és a gyártók egyre több eszközükbe integrálják a technológiát, így az emberek egyre inkább élvezhetik mobilitás előnyeit. Ezek növelik a hatékonyságot és a pontosságot, ha elegendő megtakarítást eredményeznek, a telepítéssel és üzemeltetéssel járó költségekhez képest, akkor gazdaságosnak mondható a hálózat. A nyereség pedig arra ösztönzi a többi versenytársat is hogy ruházzanak be az új rendszerbe. A megbízhatóságot nézve, a rézvezeték korrodál, és

mivel nem megfelelően használják, ezért megbízhatatlan. A nem megfelelő használat alatt a rossz elhelyezést és a sérüléseket értjük. Az időjárási viszonyok is kedvezőtlen hatással lehet az épületek közt kifeszített vezetékekre, de ugyanúgy fenyegeti a föld alatt elvezetett vezetékeket is. Ugyanakkor a vezeték nélküli hálózat jelentősen csökkenti az ilyen nemű problémák lehetőségeinek körét. A teljesítmény szempontjából viszont az előny a vezetékes testvért illeti, de a vezeték nélküli összeköttetés tartalékként még akkor is használható. Az együttes alkalmazás egy erős, megbízható rendszert hoz létre. Összefoglalva tehát a vezeték nélküliséggel az ember kiélvezheti a mobilitást, mindenhol létesíthet kapcsolatot ahol, mobil hozzáféréssel rendelkezik. Ezen kívül persze a pontosság, hatékonyság, és a megbízhatóság sem egy elhanyagolható tulajdonság, főként a vállalatok számára.

A vezeték nélküli hálózatok biztonsága

Veszélyeztető tényezők

A vezeték nélküli hálózatok biztonságát fenyegető veszélynek számos formája van, ilyen a jogosulatlan hozzáférés, a forgalommonitorozás, és a szolgáltatás megtagadásra irányuló támadások. A hackerek például, információkat lophatnak a vállalatoktól, engedély nélkül hozzáférhetnek alkalmazásokhoz, sőt akár a hálózat működését is nagyban akadályozhatják.

Forgalommonitorozás

Akár egy tapasztalt hackertől, akár egy kezdő lehallgatóig, akit snoopernek is nevezünk, könnyedén monitorozhatja a védelemmel el nem látott, vezeték nélküli hálózaton keresztül továbbított adatcsomagokat. Léteznek erre különböző szoftverek, ilyen például az AirMagnet, mely képes megmutatni a továbbított adatcsomagok tartalmát. A jogosulatlan hozzáférőknek nem kell a közvetlen közelben tartózkodni, hisz a vezeték nélküli hálózat hatósugarán belül, bárhonnan a hálózatot használó területtől akár 100 méterre is képesek monitorozni a tranzakciókat. Megszerzik, a felhasználóneveket, jelszavakat, és további kényes adatokat és azokat közzéteszik az interneten, vagy csak más visszaéléseket

követnek el vele. A problémára az a megoldás, hogy titkosítanunk kell a bázisállomás és a vezeték nélküli hálózati eszköz között. Ez az adatbiteket alakítja át egy a titkosításra jellemző kulcs szerint, így a hackerek nem tudják visszafejteni az elcsípett adatokat.

Jogosulatlan hozzáférés

A hálózat üzemeltetőinek kellő óvintézkedései nélkül, a vezeték nélküli hálózathoz, bárki hozzáférhet akár az épületen kívül is, épp úgy, mint a hálózat monitorozás esetében. Akár egy közeli padon ülve is hozzáférhetnek az épület belsejében működő bázisállomáshoz, és a megfelelő védelem hiányában, minden akadály nélkül hozzáfér a szerverek tartalmához, és a vállalati alkalmazásokhoz. Ez olyan mintha behatolt volna az otthonunkba vagy besurrant volna az irodába és ott férne hozzá féltve őrzött adatainkhoz.

Az esetek nagy többségében, ha csak egy város vezeték nélküli lokális hálózatait nézzük, több mint 25% -a csak a gyári beállításokkal működteti, bázisállomásait, eszközeit, így nem nehéz hozzáférni az alkalmazási szerverekhez. A védelem hiánya következtében, nagyon könnyű hozzáférni a merevlemezek adataihoz, és a felhasználói erőforrásokhoz az internet-összeköttetésen keresztül.

A mai operációs rendszerek, a nyilvános vezeték nélküli hálózatokhoz nagymértékben megkönnyítik a csatlakozást, és ezen keresztül azt is, hogy a lokális hálózathoz csatolt bármely más laptophoz eljuthat. Ilyenkor játszik, nagy szerepet a firewall (tűzfal), hogy megnehezítse a merevlemezünkhöz való hozzáférést.

Az imént említett biztonsági intézkedésekkel sem lehetünk biztosak dolgunkban, hisz, komoly veszélyt jelenthetnek a csaló hozzáférési pontok (rogue access point) csatlakoztatása a hálózathoz, mely engedély nélküli hozzáférési pontot jelent. Ezeket létrehozhatja akár egy a biztonsági előírásokat figyelembe nem vevő felhasználó, de a hacker is hozhat létre ilyet az épületen belül, direkt arra a célra, hogy védelem nélküli hozzáférési pontot biztosítson. Mivel semmilyen titkosítást nem alkalmaz, ezért alaposan kihasználható, bárki könnyedén hozzáférhet a vállalati hálózathoz, illetve alkalmazásokhoz, akár az

utcáról is. Erre megoldást sajnos csak a folyamatos megfigyelés jelent, az üzemeltetőnek kell vigyáznia, hogy ne tudjanak csaló hozzáférési pontot létrehozni és ez nem csak a vezeték nélküli hálózatokra igaz.

A kölcsönös hitelesítés a klienseszközök és a hozzáférési pontok között megelőzhetik az engedély nélküli hozzáférést. A hitelesítéssel azonosíthatja magát a személy vagy eszköz, így olyan eljárásokat kell implementálni a vezeték nélküli hálózatba, ami nemcsak a klienseszközök, de a bázisállomások azonosságát is igazolja. A felhasználó jogos hozzáféréséről való meggyőződés még nem elég, hiszen a hozzáférési pontokat sem árt kapcsolókkal ellátni, hogy a csaló csatlakozási pontokat kiszűrjük.

Emberközpontú támadások

A titkosítás és a hitelesítés alkalmazása bár növeli a vezeték nélküli hálózatok biztonságát, de nem akadályozza meg a hackereket a céljuk elérésében. Gyenge pont például az ember központú támadás, melyben a hacker a felhasználó és a vezeték nélküli hálózat között egy fiktív eszközt hoz létre. A leggyakrabban a címfeloldó (ARP) protokoll ellen indítanak emberközpontú támadást, mert ezt az összes TCP/IP hálózat használja, ezen keresztül ellenőrzést szerezhet a vezeték nélküli hálózat felett. Az ARP protokollt a hálózati interfészkártya, a célállomás hálózati interfészkártyájához rendelt fizikai cím megszerzéséhez használja. A kártya fizikai címe köztudottan megegyezik a közeghozzáférés-vezérlő MAC címével, mely teljesen egyedi, minden eszköznél különböző és a gyártó helyezi azt el. Az alkalmazásszerver ugyan ismeri a célállomás IP címét, de a hálózati kártya fizikai címét nem, ezért az adó oldalnak az ARP tábla segítségével ki kell deríteni azt. A címhez úgy jut hozzá, hogy egy üzenetszórással ARP-kérést, melyben megadja a keresendő célállomás IP címét. A kérdést mindenki megkapja és az, akinek az üzenetben lévő IP cím megegyezik a sajátjával, az egy ARP választ küld, mely tartalmazza a MAC címét és az IP címet is egyaránt. Az adóállomás az elküldendő keret célállomásaként ezt a MAC címet adja meg.

Az ARP protokollt sajnos könnyen be lehet csapni, így ez nem kis kockázattal jár. A hacker egyszerűen küld egy ARP választ melyben, az ő MAC

címe szerepel a küldött IP címmel. Így az összes állomás a hálózaton belül, frissíti az ARP tábláját, ezekkel, az adatokkal. Innentől pedig az állomások a csomagokat a csaló hozzáférési pontnak küldik el, a router vagy a törvényes hozzáférési pont helyett. A hacker ezáltal számára hasznos információkhoz férhet hozzá, jelszavakhoz, felhasználónevekhez, és ezekkel a vállalati alkalmazásokba is beléphet. Az ilyen nemű támadások ellen, a gyártók létrehozták a Secure ARP-t, azaz a SARP protokollt. Ez egy speciális biztonsági csatornát hoz létre a kliensek, hozzáférési pontok és routerek között, mely figyelmen hagyja az olyan ARP válaszokat, melyek nem a csatorna másik végéről érkeznek. Így csak jogos válaszok esetében történik meg az ARP tábla frissítése.

A fenn említett protokoll (SARP) alkalmazása viszont, az összes állomáson szoftvertelepítést igényel, így nem igazán alkalmazzák például a Hot spotokon.

Szolgáltatásmegtagadás

A denial of service (DoS) felé irányuló támadás megbéníthatja a vezeték nélküli hálózatot. Ezt minden üzemeltetőnek érdemes végig gondolnia, milyen következményekkel jár, ha a vezeték nélküli hálózat működés képtelenné válik? Súlyossága a kifejtett hatástól függ, egy lakásban például, legfeljebb kellemetlenséget okoz, de egy vállalatnál ez súlyos anyagi kiesést jelenthet.

Ennek a támadásnak az egyik formája a nyers erő alkalmazása. Ilyen, amikor annyi csomagot küldünk minden állomásnak, hogy a hálózat összes erőforrását lekötjük, és a hálózatot, ezáltal leállásra kényszerítik. Az elárasztás kitalálása és megvalósítása sem okoz gondot, mert az interneten léteznek olyan eszközök, melyek használata lehetővé teszi a hackerek számára a vezeték nélküli hálózatok elárasztását. Vannak más módszerek is a szolgáltatásmegtagadásra irányuló, nyers erőt alkalmazó módszerek. Küldhet a hálózat más számítógépeiről hasznavehetetlen csomagot, ez jelentősen megnöveli a terhelést és lecsökkenti a sávszélességet.

A vivőérzékelésen alapuló hozzáférést alkalmazó hálózat leállításának egy módja, hogy a használt rádióhullámot egy erősebb jellel elnyomják, ezáltal

használhatatlanná téve, rádiófrekvenciás kártyát és a hozzáférési pontot. Az IEEE 802.11 protokoll például korlátlan ideig, elérhetővé teszi a támadó jeleknek a közeg hozzáférést. Az effajta támadás azonban, igen kockázatos, ugyanis közelről kell végrehajtani, egy nagy teljesítményű adóval. A vezeték nélküli hálózat üzemeltetői, pedig hálózat analizátor segítségével, rátalálhatnak a hackerre és azt felfedése után, a rendőrséggel együttműködve letartóztathatják.

Van azonban, hogy saját magukat is képesek megbénítani a vezeték nélküli hálózatok. Vegyük például a 802.11b hálózatot, ha zsúfolt rádiófrekvenciás tartományban működik, és mondjuk mikrohullámú sütőt, bluetooth-t vagy, más hasonlóan vezeték nélkül kommunikáló eszközt használunk, az jelentősen csökkentheti, a teljesítményt. A tényezők együttes hatásából adódóan, akár teljesen is megbénulhat a vezeték nélküli kommunikáció.

A Wi-Fi védett hálózat például egy olyan védelmi mechanizmus, mely a szolgáltatás megtagadó támadások jó célpontja lehet. A WPA egy matematikai algoritmust használ a csatlakozni kívánt felhasználók hitelesítésére, így ha a belépett felhasználó rövid időn belül két illetéktelen adatokat tartalmazó csomagot küld, a védelem leáll.

Ez ellen a támadási mód ellen, még a mai napig nem igazán létezik megfelelő megoldás, hisz az egyetlen célravezető módszer, ha gépünket egy jól elzárt, erősen felügyelt, minden nemű hálózattól, internettől mentes szobába zárjuk. Ez a módszer azonban, nem egészen kielégítő, azok számára, akiknek sok előnyük származna a vezeték nélküli, vagy akár a vezetékes hálózat alkalmazásából, ilyenek lehetnek például a nagyobb vállalatok.

Talán a szolgáltatásmegtagadásra irányuló támadás elleni, legcélszerűbb védekezés a jól kidolgozott és alkalmazott biztonsági intézkedések jelentik. Ez lehet, mondjuk egy erős tűzfal mely naprakész, vírusvédelem mely sűrűn frissített, bonyolult jelszavak használatának, és a biztonsági javítóprogramok együttese. Illetve a hálózati eszközök használat utáni leállítása.

A szolgáltatásmegtagadásra irányuló támadások úgy is kivédhetők, hogy az épületet alakítjuk a lehető legellenállóbbra a beérkező jelekkel szemben. Ennek megvalósítására vannak különböző praktikák, ilyenek a következők: Az épületben használt ablakok, legyenek réz vagy fémfólia alapú hőszigeteltek. Fémszórt

ablaküveget használjunk, redőny és függöny helyett. Fém alapú festéket használjunk a falak festésére. Az esetleges fémcsapokat tartalmazó falakban szigeteljük le azokat. Meg kell továbbá azt is vizsgálnunk, milyen nagy a jeladó hatótávolsága, és állítsuk úgy be, hogy a hackerek elhelyezkedését ne könnyítsük meg, illetve ahol el tudnak helyezkedni, ott már kellően gyenge legyen a jel, vagy akár meg is szűnjön. A hozzáférési pontokat célzó jeladó antennákat irányítsuk az épület belseje felé. Összegzésül elmondható, hogy a szolgáltatásmegtagadásra irányuló támadások ellen, tényleg nem lehet tökéletesen védekezni, ami azt jelenti, hogy fel kell készülnünk arra az esetre is ha súlyos kár keletkezik a hálózatban.

Az IEEE 802.11x alszabványai

Az eredeti, 1997-ben elfogadott IEEE 802.11 szabvány frekvenciaugrásos szórt spektrumú (FHSS) és direkt sorozatú szórt spektrumú (DSSS) fizikai réteg tartalmazza mely a 2,4 GHz-es sávban és 2 Mb/s maximális adatátviteli sebességgel működnek. Mivel ez a 2 Mb/s adatátviteli sebesség már nem túl nagy a mai piacon lévő teljesítményekhez képest, így az FHSS nem is kínál megoldást a vezeték nélküli lokális hálózathoz. Másik hátránya, hogy nem működik együtt más szabványokkal a 802.11-en belül. Előnyére válhat, hogy sokan használták a kültérben történő, pont-többpont rendszerek létrehozásánál, mivel elég jól tűri a rádiófrekvenciás interferenciát. A DSSS olyan szempontból jobb, mint az FHSS, hogy tud együttműködni a 802.11 egyik újabb fizikai rétegével, a 802.11b-vel. Így a vezeték nélküli hálózatoknál is lehetne, használni például egy laptop, amiben 802.11b van, tudna kommunikálni egy DSSS hozzáférési ponttal. Ez mind a 2 Mb/s-os adatátvitel miatt nem valósul meg, mind pedig azért, mert már nem igazán gyártanak 802.11 DSSS rádiófrekvenciás hardvereket.

IEEE 802.11.a

Az IEEE 802.11a szabványt az 1999-es év végén adták ki, 5 GHz-es sávban, maximum 54 Mb/s adatátvitelre képes, ortogonális frekvenciaosztásos multiplexeléssel működő fizikai réteg. Maximum 30 méteren belül tud, hatékonyan kommunikálni, és az 5 GHz-es sávban működik. A hardverek az 5

GHz-es sávban működő áramkörök kifejlesztésének problémái miatt, csak 2000-2001-ben kerültek piacra, ennél fogva sokkal kevesebb 802.11a–val működő vezeték nélküli lokális hálózat van a hálózatok között, mint például 802.11b –s fizikai réteggel működő. A szóban forgó szabvány nagy előnye, hogy a 12 különálló, nem átlapolódó csatornának köszönhetően, csatornakapacitása a lehető legnagyobb. A másik nagy előnye ennek a szabványnak, az 5 GHz-es sáv, mivel ez a frekvencia még mindig nem telített, ezért magasabb teljesítmény érhető el vele. A magas teljesítményhez hozzájárul az is, hogy az interferáló eszközök többsége a 2,4 GHz-es frekvenciasávban működik.

A frekvenciasáv azonban nem csak előnyt, hanem hátrányt is jelent, hiszen a korlátozott hatótávolságot is pont az 5 GHz-es sáv eredményezi. Mindez azt jelenti, hogy az 54 Mb/s –os adatátviteli sebességet, csak 30 méteres távolságon belül lehet elérni. A kis hatótávolság pedig, újabb problémát szül, hiszen így újabb hozzáférési pontokra van szükség a vezeték nélküli lokális hálózat kiépítéséhez. A 802.11a és a 802.11b összehasonlításánál, azt az eredményt kapjuk, hogy jóval nagyobb átviteli sebességre képes a 802.11a, egészen addig, míg le nem szakad a hálózattól. A 802.11b-t használó hálózatok esetében ugyanis 1-2 Mb/s-os adatátviteli sebesség akkor is elérhető, ha már a 802.11a hatótávolságán jóval kívül vagyunk. Az egyik legnagyobb problémát viszont a hálózatok kiépítésére nézve, talán az jelenti, a 802.11a, 80211b/g szabványok egymással nem kompatibilisek. A gyártók ezen azzal próbálnak segíteni, hogy több üzemmódú rádiókártyákat dobnak piacra. A 802.11a esetén a modulátorok, különböző modulációs eljárásokkal a bináris jeleket, analóggá alakítják. Az eljárások kiválasztása az adatátviteli sebességtől függ, hiszen ha 6 Mb/s-os sebesség a cél, akkor a bináris fázisbillentyűzést a BPSK-t használjuk, mely úgy reprezentálja az adatmintákat, hogy az adási középfrekvencia fázisát tolja el. Nagyobb sebességnél viszont már a QAM-ot azaz a kvadratúra-amplitúdómodulációt használjuk, mely a központi adási frekvencia amplitúdóját is modulálják a fáziseltoláson kívül.

IEEE 802.11b

Az IEEE 802.11a szabvánnyal együtt fogadják el, ez az eredeti közvetlen szórt spektrumú szabvány egy nagyobb sebességű kiterjesztése 2,4 GHz-es sávra, amely így 11 Mb/s –os adatátviteli sebességet tesz lehetővé. A hálózat kiépítéséhez és telepítéséhez szükséges eszközök, már 1999 óta elérhetők a piacon, így mára már szinte minden vezeték nélküli lokális hálózat 802.11b kompatibilis.

Az egyik nagy előnye ennek a szabványnak a hatótávolság nagysága, épületen belül akár 100 méteres távolság áthidalására is képes, ami miatt kevesebb hozzáférési pont szükséges az épület lefedésére. Hátránya viszont, hogy csak 3 nem átlapolódó csatornát biztosít a 2,4 GHz-es sávban. A 802.11 eredetileg 14 csatornával rendelkezik a hozzáférési pontok kialakítására, de minden csatorna csak a 2,4 GHz-es sáv egy harmadát használja jeltovábbításra. Az interferálás elkerülése végett pedig, sokan csak az 1-es, 6-os, és 11-es csatornákat használják, ezzel lecsökkentve a hálózat kapacitását. A 802.11b szabványt elsősorban közepes alkalmazások biztosítására használják, ilyen a webböngészés és az e-mailek küldése, fogadása. A másik hátrányt a 2,4 GHz-es frekvenciasáv miatt szenvedi el, mivel ebben a sávban rengeteg az interferáló eszköz, például a telefonok, vagy mikrohullámú sütők. Az interferencia pedig a vezeték nélküli lokális hálózatok teljesítményét jelentősen csökkenti. A 802.11b modulátorok a szórt bináris jelek sebességétől függően különböző modulációs eljárásokat használnak, a bináris jelek analóggá alakításához. Az 1 Mb/s-os adatátviteli sebesség mellett, PMD különbségi bináris fázisbillentyűzést használ (DBPSK). A 2 Mb/s-os adatátviteli sebességnél pedig, különbségi kvadratúra fázisbillentyűzést (DQPSK) használ. Ezek a modulációk, nem olyan bonyolultak, hiszen az adatfolyamban lévő bináris 1-ek és 0-k megkülönböztetéséhez, csak eltolják az adási középfrekvencia fázisát. A DQPSK –nál is majdnem ugyanaz az elv, csak négy lehetséges fáziseltolás van a két adatbites szimbólum reprezentálására.

IEEE 802.11g

A 802.11g szabvány a 2003-as évben került bevezetésre. A 2,4 GHz-es sávban biztosít maximum 54 Mb/s adatátviteli sebességet, valamint visszafelé kompatibilis a 802.11b szabványú eszközökkel. 802.11b –vel való kompatibilis működés esetén 11 Mbps maximális adatátviteli sebességen, DSSS-t használva működik. Ettől eltérően („normális" működés esetén) *OFDM* modulációs eljárást használ. A kompatibilitás a 802.11b szabványt támogató eszközök elterjedtsége miatt szükséges, így a már kiépített hozzáférési pontokhoz az új, *802.11g* szabványt támogató hálózati eszközök is képesek csatlakozni, ekkor viszont az adatátviteli sebességük maximuma értelemszerűen a kisebb teljesítményű (802.11b szabványú) hozzáférési pont maximális sebessége lesz. A *802.11g* szabványt támogató hozzáférési pontok képesek visszafelé kompatibilisen működni, így ezekhez is csatlakozhatnak a már meglévő (802.11bszabványú) adaptert használó kliensek is. Annak, hogy a két szabvány eszközei kompatibilisek egymással „hátránya" is van, az, hogy a régi eszközök nem lesznek képesek nagyobb sebességre, még ha az eszközök saját belső szoftverét (firmware) frissítenénk is. Előnye viszont, hogy a nagyobb bitsebesség elérését biztosító eszközökre való átállás, a korszerűsítés fokozatosan elvégezhető.

IEEE 802.11i

2004 nyarán fogadták el, ami nem külön kommunikációs vagy fizikai réteget határoz meg, hanem biztonsági előírásokat tartalmaz. Célja, hogy bevezetésével eltűnjenek a korábbi biztonsági hiányosságok. Adattitkosításra az *AES–t* (Advanced Encryprtion Standard) használja. Biztonsági szempontból előírja továbbá a *WPA* (Wi-Fi Protected Access) protokoll használatát.

IEEE 802.11n

A 802.11n szabvány, jelen és egyben 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. A várható sebesség ráadásul nemsokára meg fog duplázódni. Érdekesség, hogy a 802.11

a/b/g kliensek nagyobb adatátviteli teljesítményt nyújtanak 802.11n hálózatban, mint a sajátjukban. Köszönhető ez az új MIMO architektúrának (multiple input, multiple output), amely egy adott Access Point típusnál nagyobb területen biztosít ugyanakkora sebességet és sávszélességet. További előnye, hogy az a/b/g alapú VoWLAN hívások esetén kiválóbb hangminőséget és biztosabb lefedettséget jelent. A 802.11n egyébként kompatibilis a korábbi 802.11 a/b/g szabványokkal, azaz minden eddig vásárolt Wi-Fi eszköz használható az új 802.11n rendszerben, ez semmilyen szoftver vagy hardverváltoztatást nem igényel. A 2,4 GHz-es sáv túlterhelt jelenleg, 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 lapoló csatorna (frekvenciasáv) áll rendelkezésre, míg a 2,4 GHz tartományban mindössze három. A több száz mb/s-os adatátviteli sebesség elérése a csatornák dinamikus váltogatásával lehetséges, ezt hívják DFS2-nek (dynamic frequency selection)

A 802.11n rendszerek 20 illetve 40Mhz-es sávszélességben dolgoznak, a korábbi rendszerek csak a keskenyebbikben. A jelvisszaverődés is komoly gondot jelentett az a/b/g rendszerekben, amelyet a 802.11n a többcsatornás átvitellel és vétellel kompenzál. A 4x4:4 MIMO elméleti sebessége 600Mbps, amit 4 adó és 4 vevőantennával produkál, 4 adatcsatornán. A jelenleg kapható Motorola eszközök 3x3:2 MIMO felépítésűek. 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.

Együttes tesztek is készültek, azaz amikor egy térrészben 802.11 a/b/g és 802.11n kliensek voltak. Az AP átbocsátó képessége drasztikusan csökkent, összesen 60Mbps-ra, és ez 80-20%-ban oszlott meg a kliensek között az 5GHz-es sávban és 90-10%-ban a 2,4 GHz-nél. A 802.11 a/b/g kliens jobban viselkedett 802.11n AP környezetében, mint a sajátjában, nagyobb távolságban, nagyobb sebességet tudott fenntartani. Vagyis a/b/g mobil eszközök esetén nagyobb teljesítményt kapunk, ha 802.11n hálózatot építünk, köszönhetően elsősorban a MIMO adási és vételi

eljárásnak. Ha még hangot is szeretnénk átvinni (VoWLAN), az előnyök tovább szaporodnak az „n” hálózat javára.

Végül talán a legérdekesebb paraméter, a sugárzási tartomány. Megnyugtató, hogy az 5Ghzes tartományban nagyobb, a 2,4 GHz-nél pedig azonos az a/b/g rendszerekkel. Vagyis az AP-k elhelyezése egy az egyben megegyezhet az a/b/g rendszerekkel. (Vigyázat, nem a csak „b”-vel!) Sőt, még kicsit ritkábban is elhelyezhetők az új 802.11n AP-k.

Van viszont egy probléma. A 802.3af PoE tápellátása nem elegendő a többcsatornás 802.11n távoli táplálásához, a teljesítmény felvétel ugyanis meghaladja a 12,9W-ot. Vagyis a tápláláshoz drágább, nagyobb teljesítményű PoE szükséges. A Motorola új RF switch, az RFS6000 már 8 ilyen beépített PoE 802.3af+ porttal rendelkezik, azaz fel van készítve a nagyobb teljesítményű 802.11n Access Portok táplálására.

Titkosítás

Titkosítás alatt azt értjük, hogy a hálózatot lehallgató személy nem tud dekódolás nélkül információhoz jutni, mivel az adatcsomag bitjei módosultak. Mielőtt titkosítanánk az adatokat, azokat nyílt szövegnek hívjuk, ezt könnyű dekódolni akár egy, egyszerűbb hibakereső programmal is. A titkosítás folyamata, olyan titkos szöveget eredményez, melyet csak a rá jellemző titkos kulcs segítségével lehet dekódolni. Vannak szimetrikus titkosító eljárások, melyeknél ugyanazzal a kulccsal lehet visszafejteni az adatokat, mint amivel titkosították azokat, ilyen például az IEEE 802.11 szabvány által előírt WEP (wired equivalent privacy) azaz vezetékes átvitellel egyenértékű titkosítás. Ezeket főleg vállalatoknál alkalmazzák, hiszen az adó is ugyanazt a kódot használja titkosításra, mint a vevő a dekódolásra, ehhez azonban meg kell bízniuk egymásban, ami a nyilvános hálózatoknál nem valósul meg. A nyilvános hálózatoknál nem célszerű tehát a szimetrikus titkosítás használata, hiszen a hacker könnyedén megszerezheti a kulcsot. Hatékonyabbá lehet tenni, azzal hogy minimalizáljuk az újrafelhasználás számát, tehát minél gyakrabban lehetőleg minden új keret küldésénél megváltoztatják. Csökkentik tehát a hálózat feltörésére adódó lehetőséget, hisz a hackernek nagyon kevés ideje marad a kulcs megszerzése után, ha egyáltalán marad. A

szimetrikus titkosítási mechanizmusoknak tehát hatékony kulcskiosztó eljárásokat kell alkalmazniuk.

A nyilvános kulcsú titkosítás aszimmetrikus kulcsokat használ, azaz a saját kulcs titkos, a de a nyilvános kulcsot bárki ismerheti. Ezzel a kulcskiosztási módszerrel, sokkal hatékonyabb titkosítási és hitelesítési mechanizmusok válnak elérhetővé. A legfontosabb követelmény ezeknél a titkosításoknál, hogy egymáshoz tartozó saját és nyilvános kulcsból álló kulcspár kell, hogy biztosítva legyen. Tehát ha az adóállomás a küldendő adatokat nyilvános kóddal titkosítja, azt a vevőállomásnak saját kóddal kell dekódolnia, és mindennek fordítva is igaznak kell lennie, de az már a küldő fél hitelesítésére szolgál.

A saját kulcsot minden állomás megtartja magának, senkinek nem adja ki annak érdekében, hogy a titkosított információ feltörését, megakadályozza. Így a folyamat biztosítja tehát, hogy nyilvános kulcs segítségével titkosított adatokat küldjön minden állomás, egy további állomásnak. Ez a fajta titkosítási eljárás igen jól használható a küldendő adatok titkosítására, hiszen a leendő vevő állomások szabadon hozzáférhetnek a nyilvános kulcshoz. Mivel minden saját kulcshoz tartozik egy nyilvános kulcs, ezért ha egy állomás új saját kóddal áll elő, annak nyilvános párját közzéteheti akár a hálózaton, akár egy honlapra.

WEP működése, problémái

A WEP egy a MAC-rétegben implementált, hitelesítési és titkosítási szabvány az IEEE 802.11-nek. A hozzáférési pontokat és hálózati kártyákat gyártó cégek termékeinek, túlnyomó része támogatja ezt a szabványt. A vezeték nélküli hálózatok, védelme érdekében, használjuk ki a WEP által nyújtott lehetőségeket.

Amikor a hálózat üzemeltetője aktiválja a WEP-et azzal az RSA által kifejlesztett bizonyos RC4 adatfolyam titkosítóval, titkosítja az interfészkártya minden egyes adatmezőjét a 802.11 keretnek, azaz a törzsét és a redundanciakódot. Tehát a küldő állomás a WEP segítségével kódolja a küldendő adatfolyamot, míg a vevő állomás dekódolja azt. Ez a folyamat azonban csak a 802.11 szabvánnyal működő állomások közt valósul meg, ugyanis ha az elküldött adat vezetékes oldalra kerül, akár két közé, akkor a WEP érvényét veszti.

A titkosító folyamat alatt a WEP az adóállomás felhasználója által megadott, titkos kulcshoz, egy 24 bites véletlenszerűen előállított inicializáló

vektort rendel, ez meghosszabbítja a titkos kulcs életét, mivel az IV minden keret küldésekor megváltozik. A WEP az inicializáló vektor értékét adja kezdőértékként, egy pseudo véletlenszám-generátornak, mely a keret adatmezőjének és egy 32 bites integritás-ellenőrző érték együttes hosszával megegyező hosszú kulcssorozatot állít elő.

Az integritás-ellenőrző értéket (Integrity Check Value) a vevőállomás mindig újraszámítja, és összehasonlítja azzal az értékkel, amit az adóállomás küldött, ha nem egyezik, akkor a küldés ideje alatt, lehetséges, hogy illetéktelen módosítás történt. Ekkor a vevőállomás, két eset közül valamelyiket teszi, vagy automatikusan visszautasítja a keretet, vagy a vevőállomás felhasználóját értesíti, és rá bízza a döntést. Az adatok visszafejtésére a WEP ugyanazt a titkos kulcsot használja, mint ahogy a titkosításra. A rádiófrekvenciás hálózati interfészkártyákban és a hozzáférési pontokon ugyanazt a kulcsot kell hát beállítani, még pedig az összesnél manuálisan.

A WEP mielőtt megkezdené az adatátvitel, egy bitenkénti XOR műveletet hajt végre, az adatmező és az ICV-érték valamint a kulcssorozat együttes bitsorozatára, és ennek eredményeként előáll a titkosított adat. A szóban forgó protokoll a keret törzsének első néhány bájtjában, mindenféle titkosítás nélkül helyezi el. Ezt és a felhasználó által megadott osztott titkos kulcsot használja, a vevőállomás arra, hogy dekódolja a keret törzsében levő adatmezőt. Az adóállomás a legtöbb esetben különböző inicializáló vektort használ, bár ezt szabvány nem írja elő. Ezzel mégis nagyobb védelmet biztosít az adatok megóvásához, és megnehezíti az illetéktelen hozzáférők dolgát. Ha a visszafejtés után a keretek eleje megegyezik, az olyan adatmintát eredményezne, melyet a hackerek a titkosító algoritmus feltöréséhez használnának.

A WEP problémái: mivel az inicializáló vektorok viszonylag rövidek, a kulcsok pedig állandóak, ezért a WEP könnyen sebezhető. A 24 bites inicializáló vektor miatt, lehetségessé válik, hogy a különböző adatcsomagok továbbításánál, ugyanazt az inicializáló vektort használja. Rosszabb a helyzet, ha egy nagyméretű, terhelt hálózatról beszélünk, mert ott egy órán belül is előfordulhat az ismétlődés. Ezt a problémát az RC4 titkosító algoritmus miatt, nem is lehet orvosolni. Ha a hacker sok olyan keretet gyűjt össze, mely ugyanazon az inicializáló vektoron

alapszik, rájöhet az osztott kulcsra, vagy kulcssorozatra. Ezek segítségével pedig, már nem lesz nehéz dolga, hogy visszafejtse a keretek tartalmát. Ez még nem minden a statikus tulajdonságú osztott titkos kulcsok miatt, még több veszély fenyegeti a hálózatot, ugyanis a 802.11 szabvány nem támogatja a kulcsok állomások közti cseréjét. Az emberek nagy többsége, hónapokig, vagy akár évekig is ugyanazt a kulcsot használja. Ezáltal lehetőséget és időt biztosítva a betolakodók általi forgalommonitorozásra.

A WEP hibái ellenére, azért több biztonságot nyújt, mint egy szabad hozzáférésű hálózat. Kutatások igazolják, hogy felhasználók közül elég sokan használnak protokoll analizátort, ilyen például az AirMagnet, ezzel kiszűrik a WEP-et sem használó vezeték nélküli hálózatokat. Az ilyen hálózatokra, könnyedén csatlakoznak, és használják az ottani erőforrásokat. Mindez a WEP használatával, elkerülhető főként a kisebb méretű hálózatoknál. A legtöbb illetéktelen személy távolt tartható, de nem mindenki van, aki ki tudja használni a WEP gyengeségét főleg a nagyobb kihasználtságú hálózatoknál.

Ideiglenes kulcsmegszorítási protokoll, WEP2, TKIP, AES

Az IEEE 802.11i szabvány, fejlesztéseket tartalmaz, melyek a vezeték nélküli lokálishálózatok biztonságára vonatkoznak. A fejlesztések közül az ideiglenes kulcsmegszorítási protokoll (Temporal Key Integrity Protokoll) az egyik, melyet WEP2-nek is nevezetek. A TKIP által alkalmazott változtatás, megoldja a kulcs újrafelhasználás problémáját, így nem csoda hogy a gyártók termékeiből nem marad ki opcióként. Működése egy 128 bites kulcs megosztásával kezdődik, mely a kliensek és a hozzáférési pontok közt történik. Ez a protokoll a kliens MAC címét egyesíti, az ideiglenes kulccsal, és egy 16 bájtos inicializáló vektort ad, így jön létre az adatok titkosítására szolgáló kulcs. Ezzel a pár lépéssel biztosítja számunkra a TKIP, hogy minden állomás más és más kulcsot fog kulcssorozatot fog használni. Mint a WEP a TKIP is RC4 algoritmust használ. Igazából nem sok különbség van a már elmondottakon kívül a WEP és a TKIP között, csak annyi hogy a TKIP minden 10000 csomag után módosítja az

ideiglenes kulcsot, ezzel a dinamikus kulcskiosztással növelve a hálózat biztonságát.

A TKIP egy igen jól alkalmazkodó protokoll, mert egy javítóprogrammal át lehet térni rá a már meglévő WEP alapú hozzáférési pontokról, rádiófrekvenciás interfészkártyákról. A TKIP -et is használó eszközök, képesek együtt működni WEP -es eszközökkel, mindenféle fenntartás nélkül. Minden elmondott ellenére, ez sem bizonyul egy kielégítőnek mondható titkosítási eljárásnak.

A 802.11i szabvány azonban, nem csak a TKIP protokollt, hanem a magas szintű titkosítási szabványt az AES -t is tartalmazza. Az AES már nem a jól megszokott RC4 algoritmussal dolgozik, hanem a Rine Dale titkosító rendszerrel, mely rendkívül erős. Ezt a titkosítási protokollt, sokan nemcsak hogy kielégítőnek, de szinte feltörhetetlennek is tartják. Mindez a 802.11i szabványban a TKIP felett használható opcióként van integrálva. Az AES -nek azonban, nem csak előnyei vannak, talán egyetlen hátránya hogy nagyon nagy feldolgozási teljesítményt igényel, és ezt a piacon lévő termékek közül kevés tudja teljesíteni. Ez az oka annak, hogy amely vállalat alkalmazni szeretné az AES protokollt, azoknak fejleszteniük kell a vezeték nélküli lokális hálózatban már meglévő és működő eszközeiket. Mivel a működéshez koprocesszor is szükséges, így a hardverek lecserélése is elengedhetetlen.

Wi-Fi védett hozzáférés

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

A Wi-fi Szövetség által létrehozott WPA tette lehetővé a biztonságos vezeték nélküli hálózati eszközök fejlesztésének megkezdését, amíg az IEEE 802.11i csoport befejezi a szabvány elkészítését. A Wi-fi Szövetség ekkora már előkészítette a WPA2 szabványt is, ami már az IEEE 802.11i szabvány végleges vázlatára épült, ezért az alkalmazott jelölések a keret mezőkben különböznek a

802.11i szabványban alkalmazottaktól, hogy elkerüljék az inkompatibilitásokat az egyesített WPA/WPA2 elkészítésekor.

Az adat titkosítás az RC4 adatfolyam-titkosítóval történik, 128-bit kulcs használatával és egy 48-bites inicializáló vektorral (IV). A legfontosabb fejlesztés a WPA belül a WEP -hez képest a TKIP bevezetése, amely dinamikusan változtatja az alkalmazott kulcsokat. Ezzel hidalva át a jól ismert kulcs-megszerzéses támadást.

A hitelesítésben és titkosításban történt fejlesztéseknek köszönhetően a WPA -ban nagymértékben javult a letöltött adatcsomagok integritása. A jóval biztonságosabb üzenethitelesítési kód (Message Authentication Code) a WPA -ban, egy "Michael-algoritmus" -nak nevezett eljárás, amely tartalmaz egy keret számlálót, mellyel megelőzi a visszajátszásos támadás végrehajtását.

A kulcsok és az IV -k 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 illesztőkkel is. Ám a Michael-algoritmus viszonylagos gyengesége miatt a WPA tartalmaz egy különleges számláló-mechanizmust (CCMP – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), amely érzékeli a TKIP törési kísérleteket, és ilyen esetben ideiglenesen blokkolja a kommunikációt a támadó gépével.

WPA2-be tehát beépítették a 802.11i. szabvány főbb jellemzőit, főleg a TKIP -t és a Michael algoritmust, továbbá egy új AES alapú algoritmust, a CCMP -t, mellyel teljesen biztonságossá tették. Így 2006. március 13.-tól kezdődően gyártott minden vezetéknélküli eszköz, kötelezően a WPA2 szabvány szerint készült, tehát „Wi-Fi” jelöléssel ellátott. A Microsoft Windows XP WPA2 támogatása hivatalosan 2005. május 1-jétől kezdve létezik.

Az osztott (Pre-shared) kulcs módot (PSK) azon otthoni és kisirodai felhasználóknak fejlesztették ki, akik nem tudnak megengedni, árából és bonyolultságából adódóan egy 802.1x kiszolgálót. Mindegyik felhasználónak kell egy összetett jelszó a hálózat eléréséhez. A jelszónak 8-63 darab nyomtatható

ASCII karakterből vagy 64 darab hexadecimális számjegyből (256 bit) kell állnia. A jelszó a felhasználó számítógépén tárolódik, amivel a legtöbb operációs rendszer alatt elkerülhető az ismételt begépelés. A jelszót a Wi-fi elérési pontban is tárolni kell. Megnövelhető a biztonság egy PBKDF2 kulcs-generálási funkció használatával. Természetesen a legtöbb felhasználó tipikusan gyenge jelszót ad meg, kitéve a hálózatot a jelszótöréses támadásnak. Ez legjobban úgy kerülhető el, ha a használt jelszó legalább, 14 teljesen véletlenszerű karakterből áll WPA és WPA2 alkalmazása mellett.

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

Néhány gyártó úgy próbálja meg kiküszöbölni a gyenge jelszavak megadását, hogy a telepítés során, egy program vagy hardver interfész által automatikusan létrehoz egy megfelelő erősségű jelszót, ilyen program például Atheros JumpStart.

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

Virtuális magánhálózatok

Nyilvános hálózaton (például Interneten) keresztül megvalósított, titkosított hálózati kapcsolat, amellyel az ügyfél számítógépe vagy akár egy teljes fiókirodai hálózat hozzáférhet a központi, belső vállalati internetre csatlakozó erőforrásokhoz.

A virtuális magánhálózat nem más, mint egy, az Interneten keresztül kiépített titkosított csatorna. Ha a cég rendelkezik egy állandó, nagy sebességű internetes kapcsolattal, a felhasználók a VPN kiszolgálón keresztül csatlakozhatnak a belső hálózatra.

Nincs szükség modemek használatára, az egyidejű hozzáférések számát csak az erőforrások korlátozzák, csak a kapcsolat sávszélessége lehet korlátozó

tényező. A felhasználó bármelyik internet szolgáltatónál, helyi tarifával csatlakozhat a világhálóhoz. A VPN másik alkalmazási területe az alhálózatok összekapcsolásához kötődik. A VPN használatával a központi hálózat folyamatosan elérhető, a VPN kiszolgáló állandó kapcsolattal csatlakozik az Internetre. A fiókiroda internetes kapcsolata lehet állandó vagy időszaki is, használhatjuk a fiókiroda nagy sávszélességű hozzáférését. A fiókiroda átjárója pedig igény szerint automatikusan felépíti a VPN kapcsolatot, és elérhetővé teszi a vállalati hálózatot, mindezt gyorsan és olcsón.

Hitelesítés

A hitelesítés fontos szerepet tölt be, a vezeték nélküli hálózatokban, hiszen így a vezetéknélküli hálózat, és a kliens egyaránt azonosítja magát. A hitelesítéshez, azonban szükség van egy távoli hitelesítő szerverre, például egy RADIUS -ra mely távoli hitelesítő tárcsázó felhasználói szolgáltatást jelent.

Az IEEE 802.11 szerinti hitelesítés gyenge pontjai

A WEP nem engedélyezi a hitelesítést, csak és kizárólag a rádiófrekvenciás hálózati kártyáknak a hozzáférési pontok felé. Mivel nem engedélyezett más hitelesítési út, ezért a hackerek, könnyedén eltéríthetik ezzel megakadályozva a folyamat befejezését. Egy kliens aktívvá válása után, megkeresi az átviteli közeget, majd megpróbál a hozzáférési ponttal társulni. A kapcsolat csak akkor jöhet létre, ha a két fél SSID -je (szolgáltatáskészlet-azonosítója) egyezik. Az egyik legnyilvánvalóbb támadási felület az SSID titkosítás nélküli küldése, hiszen könnyen lehallgathatók a csomagok. A hacker pedig a jelzőkeretben levő SSID segítségével hitelesítheti magát a hálózatban. Vannak olyan eszközök a piacon, melyek már nem broadcast -tal küldik el az SSID -t, de még így is sebezhető a rendszer, mert a kliens általa a hozzáférési pontnak küldött társulást kérő keretből.

A szabvány alapbeállítás szerint nyílt rendszerű hitelesítést ír elő, tehát a hozzáférési pont bármilyen hitelesítési kérelmet elfogad. A csatlakozni kívánó

kliens egyszerűen küld, egy kérést tartalmazó keretet, és ha megfelelő SSID -vel rendelkezik akkor a hozzáférési pont megadja az engedélyt.

Az IEEE 802.11 szabvány tartalmaz, egy úgynevezett osztott kulcsos hitelesítést, mely jóval fejlettebb. A folyamat végéig a következők zajlanak: a kliens egy hitelesítési kérelmet tartalmazó keretet küld. A hozzáférési pont válaszol, egy olyan kerettel, mely egy speciális karaktersorozatot, a felkérő szöveget tartalmaz. Ezután a kliens a közös WEP titkoskulccsal titkosítja a felkérő szöveget, és visszaküldi azt. A hozzáférési pont pedig a visszafejti a közös titkos kulcs segítségével. Ha az így kapott szöveg egyezik az eredeti küldött szöveggel, akkor hitelesíti a klienst. Ez a módszer már alkalmasabb, a hitelesítés elvégzésére, de csak azt bizonyítja, hogy a kliens a megfelelő WEP kulccsal rendelkezik.

MAC-szűrők

A MAC szűrés használatánál a hozzáférési pont, minden érkező keretben megvizsgálja a forrás MAC címét. Az olyan kereteket visszautasítja, mely küldőjének MAC címe nincs az adminisztrátor által összeállított és beprogramozott listán.

Ez egy egyszerű hitelesítési módszer, melynek vannak gyenge pontjai. A WEP a keretben a MAC címmezőt, nem titkosítja, tehát ha a hacker lehallgatja a forgalmat, érvényes MAC címhez juthat. Innentől már csak át kell programoznia a rádiófrekvenciása interfészkártyát, hogy a MAC címe megfeleljen az elvárásoknak. Ezzel a jogosulatlan felhasználó is valódi felhasználónak álcázhatja magát. A hitelesítés ez a módja nem nagyon kedvelt a hálózatot felügyelők körében, hisz manuálisan egy táblázatba kell-e tárolni az összes jogosult felhasználó MAC címét. Az új felhasználó felvitele sem egyszerű, hiszen meg kell tudni a MAC címet, majd az bevinni a táblázatba és elvégezni a megfelelő módosításokat, hogy a leendő felhasználó hozzáférjen vezeték nélküli lokális hálózathoz. Ez a megoldás nem nagyon kedvelt a vállalatoknál, nagyobb hálózatoknál, de az otthoni vagy kisebb irodai hálózatokba való alkalmazásra kiváló.

Nyilvános kulcsú titkosításon alapuló hitelesítés

A nyilvános kulcsú titkosítás, nem csak az információkat, adatokat kell védeni a jogosulatlan hozzáférőktől, de hitelesítésre is használható. Erre is akkor lehet szükség, ha a hálózat védett oldalára szeretnénk csatlakozni, és ezt a hozzáférési pont, vagy a hozzáférés vezérlő engedélyével szeretnénk ezt elérni. Az állomások hitelestése először egy szövegrész, saját kulccsal való titkosítással kezdődik. A vevőállomás, a kapott szöveget az adóállomás nyilvános kulcsával fejti meg, ha a kapott szöveg egyezik az előre meghatározott szöveggel, akkor nyilvánvalóvá válik az adóállomás érvényessége.

Az IEEE 802.1x szabvány, és azon alapuló működés

Ez a szabvány hatékony keretet biztosít az automatikus hitelesítésre, ellenőrzésre, és a dinamikusan változó titkosító kulcsok használatára. Az EAP protokollt használja, és több hitelesítési eljárást is támogat, egyszer használt jelszavakat, token kártyákat, és akár a nyilvános kulcsú hitelesítést is.

A hitelesítési folyamat a vezeték nélküli klienseszköz, szeretne kapcsolatot létesíteni, a vezeték nélküli bázisállomással, azaz a hitelesítővel. A hitelesítő lehetővé teszi az egyik portján keresztüli hitelesítő szerverhez való tovább haladást. Míg a hitelesítő szerver nem igazolta az azonosságát, a bázisállomás minden, a klienstől érkező további adatforgalmat blokkol. A hitelesítés után, a hitelesítő szerver által közölt jogok alapján, a bázisállomás megnyitja portját, a klienstő érkező más típusú adatforgalomnak is. A lépések tehát a következők: először a kliens EAP kezdőüzenetet küld. Ez indítja el a hitelesítésig folyó üzenetváltást. A bázisállomás, erre egy kéréssel válaszol, melyben az azonosítóra kíváncsi. A kliens elküldi azonosítóját, egy EAP válaszban. A hitelesítő szerver, egy speciális algoritmus segítségével leellenőrzi a kliens azonosságát, és elfogadó, vagy elutasító választ küld a bázisállomásnak. A bázisállomás a válasz mikéntjétől függően, válaszol a kliensnek. Ha a hitelesítő szerver elfogadó választ küld, akkor a bázisállomás a kliens portját hitelesítettnek veszi, és más adatot is továbbít.

Ez a protokoll tehát hatékony hitelesítést biztosít, még akkor is ha nem használ titkosítást. Ha a 802.1x hitelesítő szervert dinamikus kulcscsere végrehajtására konfigurálták, akkor viszonykulcsokat is küldhet az elfogadó üzenettel. Ezeket a viszonykulcsokat, olyan EAP üzenet elkészítéséhez használja a bázisállomás, melyet közvetlenül a hitelesítés után továbbít. Az üzenet tartalmét használja fel a kliens, az olyan titkos kulcsok meghatározására, melyek felhasználhatók. A titkos kulcsok közt a kliens, megfelelő időközönként váltogat, a lehallgatás következtében lehetséges kulcsfeltörés elkerülése érdekében.

Hitelesítés típusok

Az IEEE 802.1x szabványban nem szerepelnek, a tényleges hitelesítési mechanizmusokat. A szabványon alapuló hitelesítéskor ki kell választani az EAP egy típusát, mely megadja a hitelesítés mikéntjét. Választhatunk az EAP szállítási réteg biztonság, az EAP alagutas szállítási réteg biztonság közül, de akár a CISCO könnyűsúlyú EAP módszerét is választhatjuk. A típusokat támogató szoftver futhat, a hitelesítő szerveren, vagy a kliens operációs rendszerén.

Biztonsági rendszabályok

Ha egy vezeték nélküli hálózatot biztonságossá akarunk tenni, akkor az első lépesek közt kell lennie, a hatékony biztonsági rendszabályok kidolgozása és az azt kikényszerítő, megfelelő eljárások alkalmazása. Ezt megtenni, csak az elvárásokkal szembeni felmérésekkel lehet, illetve aztán az ennek megfelelő védelmet kell létrehozni. Alapvető igény például egy jó titkosítás, ez a kisebb hálózatokban, és lakásokban lehet például WEP, a nagyobb irodai alkalmazásoknál azonban inkább egy komolyabb titkosítási eljárást kell használni, ilyen lehet a WPA. A megfelelő hitelesítési eljárás megválasztása is fontos lehet, elég hatékonynak mondható például a kölcsönös hitelesítő eljárások közül a LEAP vagy az EAP-TLS (szállítási réteg biztonság).

Értékelés lépései, általános biztonsági rendszabályok

A vezeték nélküli hálózat létrehozása után, ajánlott meggyőződnünk róla, hogy eleget tesz a biztonsági elvárásoknak. Ez abban nyilvánul meg, hogy megnézzük rendelkezik e a megfelelő biztonsági mechanizmusokkal. Nem szabad a rendszertervben teljesen bízni, legjobb megoldás, ha teszteket használunk, arra hogy megbizonyosodjunk róla, a hálózatot kellőképp, megerősítettük és távol tartja az illetéktelen hozzáférőket. Ezeket a teszteket, szintén a hálózattól függően kell elvégezni, egy kis hálózatnál elég évente egyszer megbizonyosodni arról, hogy a vezeték nélküli lokális hálózatban történő változások, nem tették sebezhetővé a hálózatot. Egy nagyobb jelentőségű hálózatnál, vállalatoknál, rendszeres időközönként kell tesztelni, az időköz lehet akár fél év is.

A meglevő biztonsági rendszabályok áttekintése: Az értékelés megkezdése előtt, jó, ha megismerjük a vezeték nélküli hálózatok biztonságára vonatkozó vállalati rendszabályokat. Ennek megtételével, lehetővé válik a rendszabályok módosítására vonatkozó javaslattétel. Meg kell vizsgálnunk, például, hogy milyen engedményeket tehetünk az alkalmazottaknak, a vállalati erőforrások hozzáféréséhez. Azt is szem előtt kell tartanunk, hogy a titkosítási és hitelesítő eljárások közül, melyik mennyire könnyen kijátszható, feltörhető. A bázisállomások telepítését is felügyelet alá vonhatják, mivel érdekük hogy a telepített bázisállomások, megfelelően legyenek konfigurálva, ezáltal a rendszabályoknak megfelelő biztonságot nyújtsanak.

A hálózat üzemeltetéséért felelős személyeknek, át kell venniük a dokumentációkat, meg kell ismerniük a bázisállomások konfigurációját, épp úgy, mint a rendszer architektúráját. Ezután, meg kell tudniuk állapítani, hogy a rendszerben van-e olyan gyenge pont, vagy hiba mely sebezhetővé teszi a hálózatot a hackerekkel szemben. Ismerniük kell, minden olyan eszközt mellyel erősíthetik a védelmet, és eljárást mellyel meghatározhatják a hiba helyét. Vannak olyan vállalatok, ahol a vezeték nélküli hálózat bázisállomásait a vezetékes Ethernet hálózaton keresztül állítják be, és azon keresztül küldik el a használathoz, illetve beállítási joghoz szükséges jelszavakat. Ezzel hozzásegítik az épp esetleg a hálózatot monitorozó hackert, az erőforrásokhoz való hozzáféréshez.

Egy szintén fontos lépés lehet, a hálózatot használó alkalmazottakkal való elbeszélgetés is, hiszen így megtudhatjuk ismerik-e a biztonsági rendszabályokat. Ha ismerik is a szabályokat, még korán sem biztos, hogy be is tartják azokat, lehetséges az, hogy az általuk vásárolt bázisállomás telepítésekor nem működnek együtt a felelős osztállyal. Előfordulhat az is, hogy az alkalmazott nem csak hogy a titkosító, hitelesítő eljárásokat, illetve módszereket nem használja, hanem még tűzfala sincs.

A bázisállomások konfigurációjának ellenőrzése, a legfontosabb lépések közé tartozik. Vigyünk magunkkal megfelelő eszközöket, és a bázisállomást tartalmazó épületeket sorra járva győződjünk meg róla, hogy megfelelőek a beállítások. A központilag támogatott szoftverhez a vezetékes oldalon férünk hozzá, egy konzol segítségével. Tehát ez esetben is leellenőrizhető, hogy a biztonsági rendszabályoknak megfelelő mechanizmusokat használnak-e. A fizikai csatlakozás sikeressége után, máris biztosak lehetünk benne, hogy nem minden rendszabálynak tettek eleget, hiszen a fizikai konzolhoz rendelt portokat, a bázisállomásoknak le kell tiltaniuk. A legtöbb bázisállomásnál mégis azt tapasztaljuk, hogy ezt a beállítást elmulasztották, ezzel lehetőséget teremtve az illetéktelen hozzáférőknek, a gyári beállítás visszaállítását. A rendszerprogramok naprakészségére is ajánlott figyelmet szentelni, hiszen a friss firmware tartalmazza azokat a módosításokat, amik a titkosítás támadási felületeit megszüntetik. A bázisállomások elhelyezése is nagy szerepet játszik a védelemben, vizsgáljuk a megközelíthetőséget, antennák típusát, orientációját, a rádióhullámok terjedését. Javasolt olyan helyre tenni a bázisállomásokat, ahol nehezen hozzáférhetők, és szem előtt vannak, ilyen lehet egy jól elzárt iroda, vagy az álmennyezet feletti légtér, ahol csak létrával hozzáférhető és ez valószínűleg feltűnik az alkalmazottaknak. Az így elhelyezett eszközök csökkentik a támadások lehetőségét.

Az alkalmazottak nem törődve a biztonsági rendszabályokkal, csaló bázisállomásokat telepíthetnek irodáikba. Ezek nincsenek megfelelően konfigurálva, és nyitott nem biztonságos porton keresztül csatlakoznak a vállalati hálózathoz. Mivel ez nagy veszélyt jelenthet, érdemes rá odafigyelni. A leghatékonyabb módszer a csaló bázisállomások felderítésére, ha a hackerek által

is használt lehallgató eszközökkel végigjárjuk az épületeket. Vezetékes oldalról pedig, időről időre végig kell járni a hálózatot, az engedély nélkül használt bázisállomások felderítésére. Ezt a célt szolgálják a vezeték nélküli hálózat-felügyeleti rendszerek.

A kakukk tojások felderítésén kívül, próbáljunk meg a hackerek számára is elérhető eszközökkel hozzáférni a hálózati erőforrásokhoz. Egy WEP -vel védett hálózatba is megpróbálhatunk behatolni, vagy megnézhetjük azt is, hogy a felhasználók területén kívülről lehet-e csatlakozni a hálózathoz. Egy nyílt hálózatnál nem lesz gond, az erőforrásokhoz való hozzáférés, de egy WEP vagy egy erősebb védelmi mechanizmuson való áthatolás, már nagyobb problémát jelent.

A hálózat kiértékelése alatt, sok mindent megtudtunk, a biztonsági rések felkutatására és betömésére is szánnunk kell egy kis időt. Ezeket nagyon sok dolog okozhatja, lehet ez a rossz architektúra, a rendszabályok figyelmen kívül hagyása. A rések megtalálásához és kiküszöböléséhez, azonban nem elég egy átlag emberként, hanem egy hackerként kell gondolkodnunk. Ha így teszünk, fel tudjuk ismerni minden olyan módszert és lehetőséget, mely megkönnyíti az illetéktelen behatoló dolgát.

A rendszer gyengeségeinek maghatározása után, megkereshetjük a problémák megoldására szolgáló módszereket. A rendszabályok szigorítására való javaslat lehet, az első lépés, amit megtehetünk annak érdekében, hogy elérjük a megfelelő biztonsági szintet.

Általános biztonsági rendszabályok

A vezeték nélküli hálózatok létrehozásánál, olyan biztonsági rendszabályokat kell kialakítani, melyek az hackerekkel szemben megvédi a rendszer erőforrását. Ezt elérhetjük, sokféleképp, az alábbi sorokban ezekből a módszerekből mutatunk be néhányat.

A számunkra elérhető, lehető leghatékonyabb titkosítást kell alkalmaznunk. A gyakorlott hackereknek nem okoz gondot egy szimpla WEP –pel védett hálózatba való betörés. Ezt s titkosítási szabványt mégis, sok hálózatnál

megoldja a biztonsági problémák nagy részét, és távol tartja a jogosulatlan hozzáférőket. Nyugodtan merem kijelenteni, hogy a WEP alkalmazása minimális elvárás a mai hétköznapi hálózatokban is. Amennyiben, még biztonságosabban akarjuk érezni magunkat, akkor a statikus módszerek helyett használjuk inkább, például a WPA –t. A WPA ugyanis, a vezeték nélküli hálózatok egy olyan titkosítása, mely gyakran váltogatja a kulcsát.

A rendszerprogramok frissítése is az általános biztonsági rendszabályok része, hisz a forgalmazók gyakran implementálnak az addigi problémákat orvosló megoldásokat, az új rendszerprogramokba. Egy eszköz vétele és üzembe helyezése után, azonnal frissítsük a rendszerprogramot, ezzel kijavítva az addig létező, és ismert hibákat.

A bázisállomások fizikai elhelyezése, azon okból kifolyólag lehet fontos, hogy léteznek olyan eszközök melyeket a reset gombbal újraindítva, a gyári beállításukat nyerik vissza. Ezek sebezhető pontokat eredményeztek, melyeket csak úgy lehet orvosolni, ha a bázisállomásokat nehezen elérhetőnek, és hozzáférhetőnek kell lennie. A reset gomb nélküli kiviteleken, másképp oldják meg a visszaállítást, egy konzol segítségével RS-232 vezetéken. Az elkerülés érdekében, tiltsuk le, a konzolhoz rendelt portot. Nem szabad szem előtt hagyni a hozzáférési pontokat, ugyanis ott az igazi bázisállomást a csaló bázisállomásra cserélhetik. Ha csak lehetőségünk van rá, a bázisállomásokat tartsuk kikapcsolva, ezzel ugyanis erősen korlátozzuk az illetéktelen hozzáférés végrehajtásához rendelkezésre álló időt.

Az alapértelmezett jelszavak megváltoztatása, az alapvető biztonsági rendszabályok közé tartozik. Ne használjuk, a gyári jelszavakat, ezekhez ugyanis bárki könnyedén hozzájuthat, és sok kellemetlenséget okozhat. Érdemes egy komolyabb jelszót választani, mely nehezen kitalálható. Ezt elérhetjük a kis- és nagybetűk használata, és a különleges karakterek, szimbólumok használatával is. A jelszóváltoztatás, legyen rendszeres, és mindig győződjünk meg róla, hogy a jelszó megfelelően van titkosítva, mielőtt továbbításra kerül a hálózaton.

Ha a rendelkezésünkre álló eszközben, ki lehet kapcsolni az SSID üzenetszórást, akkor ezt tegyük meg, mivel ezzel megakadályozhatjuk, hogy a vezeték nélküli lokális hálózatok felhasználói automatikusan észleljék a körülöttük

lévő SSID-azonosítókat. A monitorozó eszközök ugyanis figyelik, a 802.11 jelzőkereteket, melyben a bázisállomás elküldi az SSID-azonosítót is. Az SSID üzenetszórás kikapcsolásával tehát, a jelzőkeretben nem lesz benne az SSID-azonosító, és így a monitorozó programok nagy része használhatatlanná válik. A tapasztaltabb monitorozókat, ez sem tántorítja el, találnak megoldást, az IEEE802.11 szabványon alapuló társítókeretből veszik ki az SSID-azonosítót.

A biztonsági rendszabályokba gyakran belefoglalják, a rádióhullámok terjedésének csökkentésére vonatkozó igényt. Az olyan erősítő tényezőkkel, és orientációval rendelkező vezeték nélküli hálózati antennával rendelkezünk, melyen a rádióhullámok terjedése csökkenthető, azzal a lefedettség is optimalizálható, de minimálisra csökkenti annak is az esélyét, hogy a kiszivárgott jeleket, bárki is lehallgassa, vagy csatlakozzon a hálózathoz.

A személyi tűzfalak használatának előnye is megnyilvánulhat akkor, ha a hacker csatlakozott a vezeték nélküli hálózathoz, és így könnyedén hozzáférhet a hozzáférési pontokon levő fájlokhoz, adatokhoz. Javasolt tehát, hogy minden felhasználó használjon személyi tűzfalat, és tiltsa meg a fájlmegosztást.

A csaló bázisállomások és az alaphelyzetbe állított bázisállomások kiszűrése és konfigurálása, nagyon fontos feladat, ezért használjunk hálózatmonitorozókat. Ha olyan bázisállomást találunk, ami nem a biztonsági rendszabályoknak megfelelően működik, azt állítsuk be és gondoskodjunk a tikosításról. Használjunk behatolás érzékelőket, mely kiszűri a hamis MAC-címeket, és a gyanús viselkedéskor gondoskodjunk a riasztásról.

A hálózat üzemeltetőinek, célszerű meggyőződni arról, hogy a felhasználók az érvényben lévő biztonsági rendszabályoknak megfelelően végzi a vezeték nélküli hálózat telepítését. Előírhatjuk, hogy melyik gyártó, mely termékeit használhatják a felhasználók, és megtilthatjuk az engedély nélkül működő bázisállomások használatát. Az engedélyezett hálózati eszközök MAC-címének nyilvántartásával, ugyanis ezek segítségével, kiszűrhetjük a csaló bázisállomásokat.

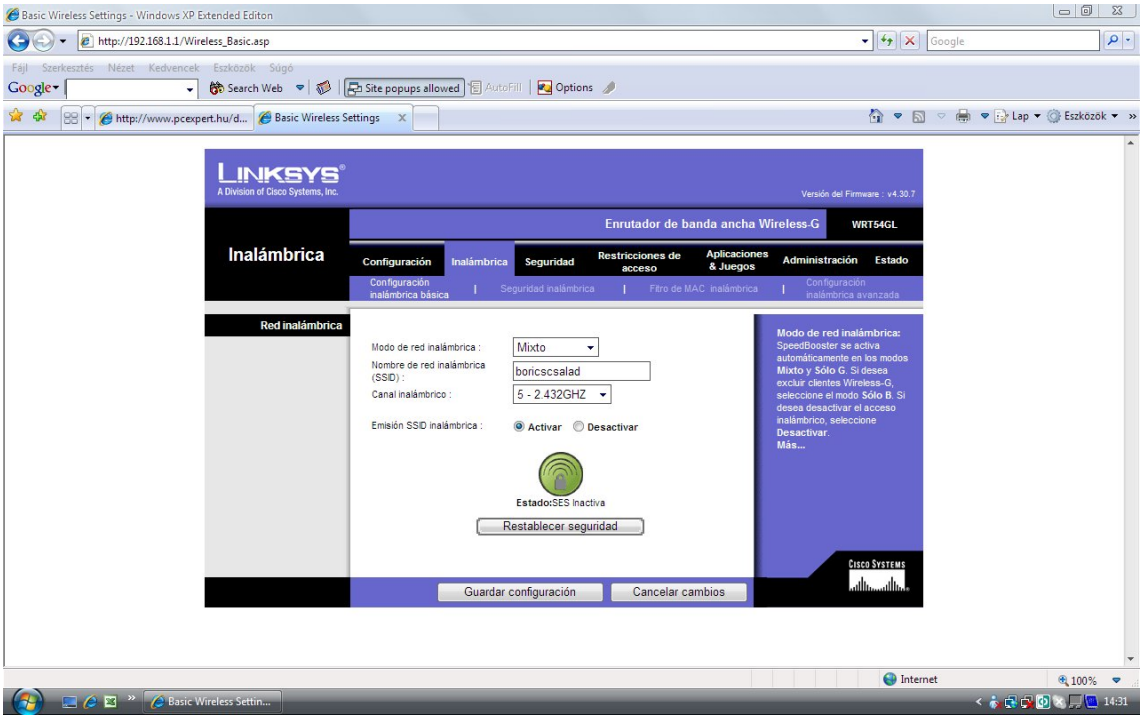
A nagyobb biztonság érdekében, használhatjuk, a demilitarizál zónát (DMZ), úgy hogy a vezeték nélküli hálózat, és a vállalati hálózat közé tűzfalat üzemelünk be. Az ilyen megoldás használatánál, minden klienst, olyan virtuális

magánhálózattal látunk el, melyet a védett hálózat elfogad. Ezzel a kis csavarral, a hackerek dolgát igen megnehezítjük, ugyanis a hálózat erőforrásainak használatához, helyesen konfigurált virtuális magánhálózatot kell használnia. Ezt a megoldást azonban csak akkor érdemes fontolóra venni, ha a felhasználók nyilvános területre is lépnek, mivel az ilyen hálózat kezelése nehéz, és teljesítménye is ingadozó.

A fenn említett néhány javaslat alkalmazásával, és betartásával igen erős, és szigorú biztonsági rendszabályokat hozhatunk létre, de a tényleges kialakításnál, azért vegyük figyelembe a valós biztonsági igényeket is.

Vezeték nélküli router néhány beállítása

Ebben a részben szeretnék bemutatni néhány beállítási lehetőségét egy Linksys márkájú, beépített hozzáférési ponttal rendelkező, vezeték nélküli routernek. A Mode –nál lévő legördülő menüből válassza ki a megfelelő hálózattípust: amennyiben 802.11g és 802.11b eszközök is vannak a hálózatán, válassza a Mixed beállítást! Ha csak 802.11g, akkor G Only, ha csak 802.11b eszközök, akkor a B Only -t! Az SSID a vezeték nélküli hálózat neve, amely alapján azonosítható. Egy vezeték nélküli hálózatban minden eszköz azonos SSID -t kell, hogy használjon. Az SSID kis-nagybetű érzékeny és legfeljebb 32 karakter hosszú lehet! Javasolt, hogy a változtassuk meg az alapbeállítást és adjunk saját nevet hálózatunknak! Channel pontnál választhatjuk ki a megfelelő csatornát, amelyen a vezeték nélküli hálózati eszközei kommunikálni fognak. A hálózatban lévő összes eszköz azonos csatornát kell, használjon! SSID Broadcast ki és bekapcsolható. Amikor a vezeték nélküli kliensek keresnek egy hálózatot, akkor az SSID alapján azonosítják. Amennyiben az ember azt szeretné, hogy az SSID sugárzásra kerüljön, válassza az Enabled állapotot. Biztonsági okokból javasolt az SSID elrejtése, ehhez válasszuk a Disabled funkciót! Miután minden beállítást elvégeztünk, ne feledjünk el menteni a Save Settings gombbal. Ha mégsem szeretnénk a beállításokon változtatni, nyomja meg a Cancel Changes gombot.



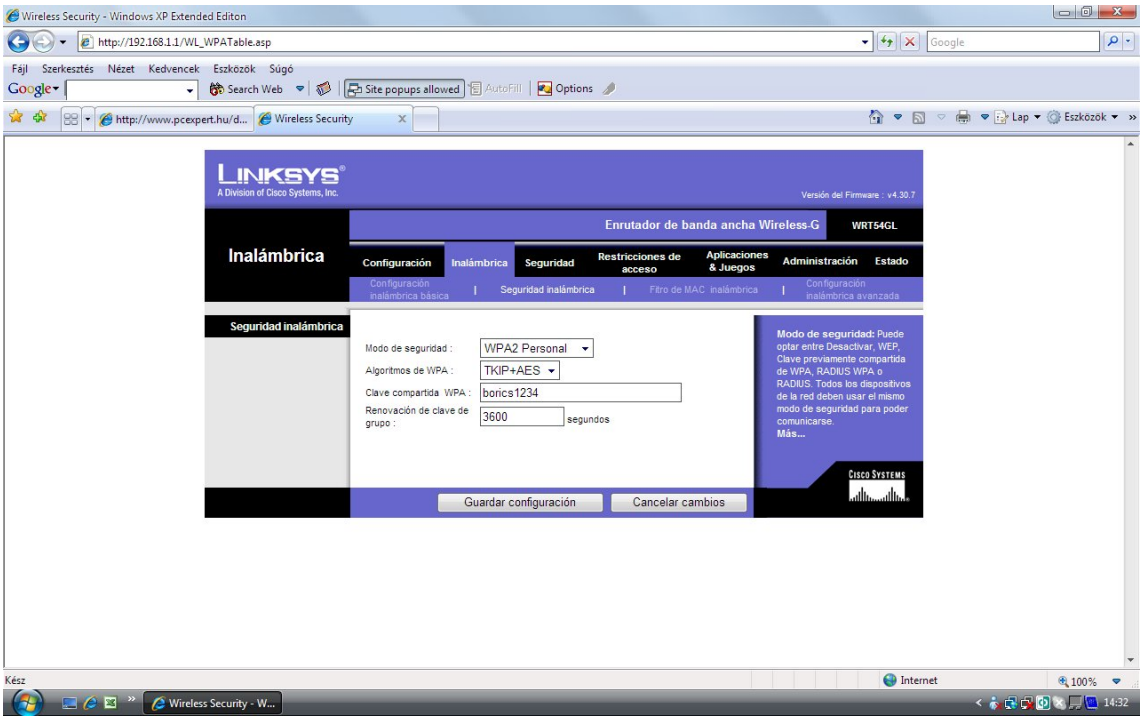
A Wireless Security ablakban állíthatóak be a vezeték nélküli hálózat biztonsági paraméterei. Eszköztől függően több titkosítási mód közül választhatunk, ezek WPA Personal, WPA2 Personal, WPA2 Mixed Mode és a WEP, illetve WPA Enterprise, WPA2 Enterprise. A beállítások befejezte után, mentsük a változásokat, vagy vonjuk vissza azokat.

A WEP egy belépő szintű titkosítási módszer, a titkosítási szintek közül a 64-bites vagy 128-bites választható. Amennyiben a felhasználó szeretne kulcsszót használni, akkor adja meg a Passphrase mezőben, majd nyomja meg a Generate gombot. Ha kézzel kívánja megadni a WEP kulcsot, akkor ezt megteheti a WEP Key 1-4 mező(k)ben. A megfelelő kulcs használatához figyelje a TX Key -t azaz, hogy hányadik sorba írta a kulcsot.

WPA Personal. Ez az eljárás két titkosítási módot használhat ezek a TKIP és az AES, dinamikus tikosítókulccsal. Válasszuk ki a használni kívánt eljárást a TKIP és AES közül. Adjuk meg a kódszót, amely legalább 8 maximum 63 karakter hosszú lehet. Ezután adjuk meg a Key Renewal (kulcs megújítási) időközt, amely meghatározza a routernek, hogy milyen gyakran cserélje a titkosító kulcsot.

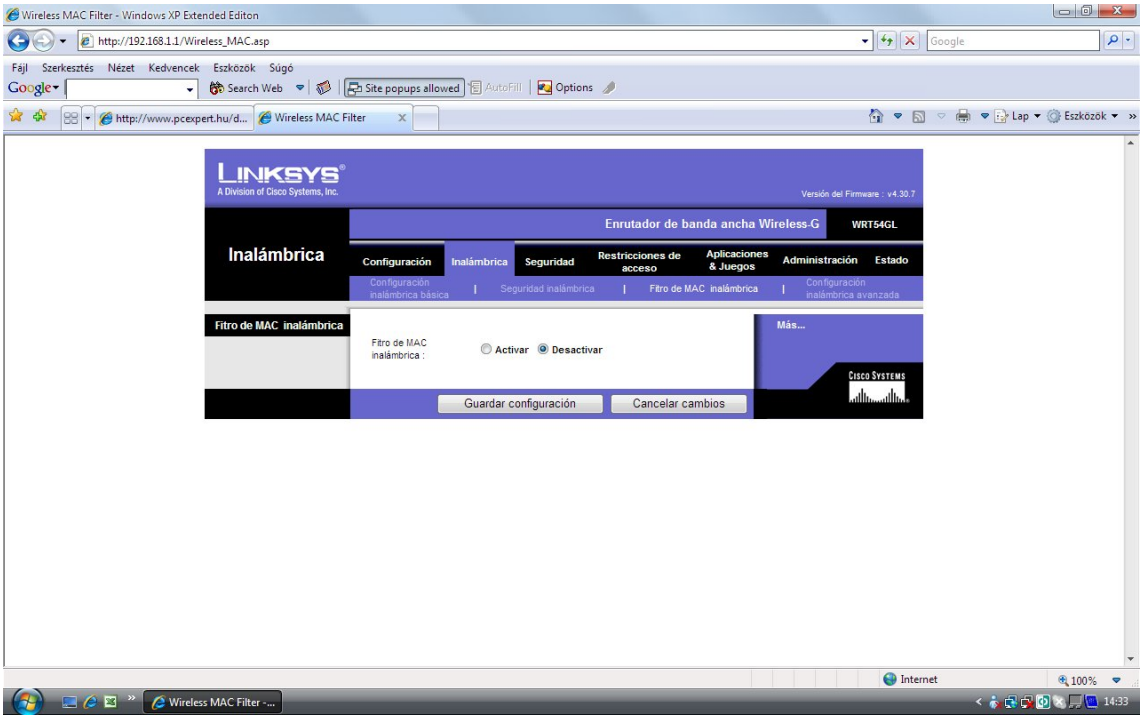
WPA2 Personal. A WPA2 esetén az AES algoritmust használjuk, dinamikus tikosítókulccsal. Adjuk meg a kódszót, amely legalább 8 maximum 63 karakter hosszú lehet.

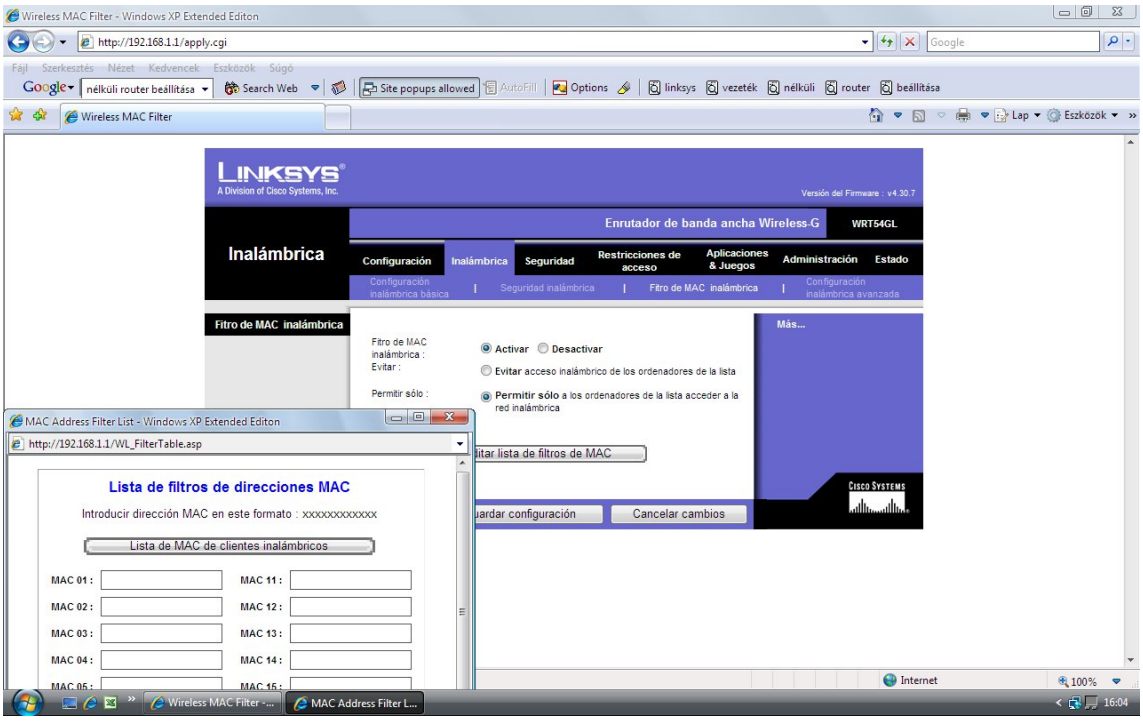
Ezután adjuk meg a kulcs megújítási időközt is.



WPA2 Mixed Mode. WPA2 Mixed Mode TKIP+AES titkosítást is használhatóvá tesz. Nem minden router támogatja ezt a funkciót. Itt is megadjuk a kódszót, amely legalább 8 maximum 63 karakter hosszú lehet, aztán a kulcs megújítási időközt, amely meghatározza a routernek, hogy milyen gyakran cserélje a titkosító kulcsot.

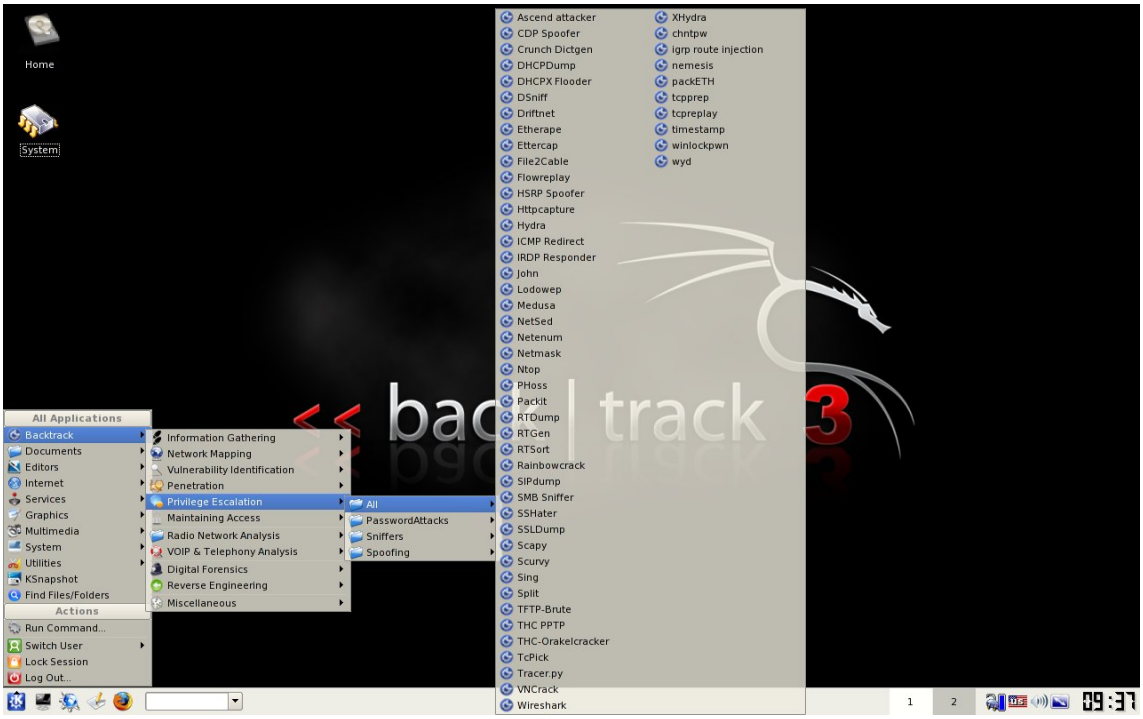
A vezeték nélküli hozzáférés szűrhető az eszközök MAC címének folyamatos figyelésével. Wireless MAC Filter. A vezeték nélküli felhasználók MAC cím szerinti szűrése lehet megengedő, ilyenkor használjuk az Enable funkciót vagy tiltó, ekkor pedig használjuk a Disable pontot. A Prevent PCs listed below from accessing the wireless network pont bekapcsolásával a lentebb felsorolt MAC címmel rendelkező eszközök nem férhetnek hozzá a hálózathoz. Ha viszont a Permit PCs listed below to access the wireless network pontot választjuk, akkor az alatta felsorolt MAC címmel rendelkező eszközök férhetnek csak hozzá a hálózathoz. Ha a Wireless Client MAC List gombra kattintunk, megjelnik mely felhasználók, mely MAC címek használatával kapcsolódnak éppen a hálózathoz. A legördülő menü To Sort by használatával különféle módokon rendezheti a táblázatot. (Kliens neve, IP címe, MAC címe). A biztonság kedvéért és hogy biztosan a legfrissebb információkhoz jussunk hozzá, nyomjuk meg a Refresh gombot, az ablak bezárásához a Close gombot. Save Settings gombbal menthetünk, a Cancel Changes gombbal visszavonjuk a beállításokat.


Wireless MAC Filter - Windows XP Extended Editon
http://192.168.1.1/Wireless_MAC.asp
Wireless MAC Filter
LINKSYS
A Division of Cisco Systems, Inc.
Versión del Firmware : v4.30.7
Enrutador de banda ancha Wireless-G
WRT54GL
Inalámbrica
Configuración
Inalámbrica
Seguridad
Restricciones de acceso
Aplicaciones & Juegos
Administración
Estado
Configuración inalámbrica básica
Seguridad inalámbrica
Filtro de MAC inalámbrica
Configuración inalámbrica avanzada
Filtro de MAC inalámbrica
Filtro de MAC inalámbrica :
Activar
Desactivar
Más...
Guardar configuración
Cancelar cambios
Internet
100%
Wireless MAC Filter -...
14:33


Wireless MAC Filter - Windows XP Extended Editon
http://192.168.1.1/apply.cgi
Wireless MAC Filter
LINKSYS
A Division of Cisco Systems, Inc.
Versión del Firmware : v4.30.7
Enrutador de banda ancha Wireless-G
WRT54GL
Inalámbrica
Configuración
Inalámbrica
Seguridad
Restricciones de acceso
Aplicaciones & Juegos
Administración
Estado
Filtro de MAC inalámbrica
Filtro de MAC inalámbrica :
Evitar :
Activar
Desactivar
Evitar acceso inalámbrico de los ordenadores de la lista
Permitir sólo :
Permitir sólo a los ordenadores de la lista acceder a la red inalámbrica
Más...
MAC Address Filter List - Windows XP Extended Editon
http://192.168.1.1/WL_FilterTable.asp
Lista de filtros de direcciones MAC
Introducir dirección MAC en este formato : xxxxxxxxxxxx
Lista de MAC de clientes inalámbricos
MAC 01 :
MAC 02 :
MAC 03 :
MAC 04 :
MAC 05 :
MAC 11 :
MAC 12 :
MAC 13 :
MAC 14 :
MAC 15 :
Cancelar cambios
Internet
100%
Wireless MAC Filter -...
MAC Address Filter L...
16:04

A BACKTRACK rövid ismertetése

A Backtrack az egyik legjobb live linux disztribúció, mely a penetráció vizsgálatra összpontosít. Nem igényel installálást, akár cd-rom –ról akár USB –ről indítható, perceken belül teljesen fel áll a rendszer, és már kezdődhet is, a platformelemzés. A nagysikerű Auditor Security Collection és a szintén elterjedt Whax disztribúciók egyesítésével jött létre. Olyan sikert ért el, hogy 2006-ban az insecure.org a Security Live Distribution alkalmazások listájának élére tette a Backtracket. A Backtrack fejlesztői az újabb és újabb verziókban, nemcsak új alkalmazásokkal lepték meg a felhasználókat, és javították az esetleges hibákat, hanem összehangolták Backtrack áthatolás vizsgálati módszereit és az értékelő kereteket, ezzel megkönnyítve a professzionális felhasználók munkáját. Rengeteg, hasznos programot, és alkalmazást zsúfoltak a Backtrack –be, ezek közül szerepel néhány az elkövetkezendőkben, egy rövid leírásban.



Information Gathering Eszközök

Gooscan

Gooscan olyan eszköz, ami automatikusan lekérdezi Google adatbázisát a kívánt információról. pl: gooscan -t www.google.com -q "blacklinux.atw" Eredmény:blacklinux.atw csak egy van, de már blacklinux 956 találat.

Archive.org

Nagyon hasznos infomációkat szerezhetünk www.arhive.org oldalról. Itt elérhetők olyan oldalak is, amit eltávolítottak valamely okból az internetről.

Host

A host utasítás használata igen hatékony módszert biztosít számunkra a távoli helyek IP -címének vagy URL -jének megállapításához.

TCtrace

TCtrace működése során TCP SYN csomag kérés alapján működik. Az egyik rendszertől a másikig vezető útvonal több lehetséges utat is követhet. Ezeket érdemes megvizsgálni. Erre az egyik legjobb program traceroute. A lassabb kapcsolatok esetén értékes információkhoz jutunk, amit figyelembe véve hatékonyabb útvonalat kereshetünk.

Itrace

Itrace működése során ICMP csomag kérés alapján működik. Az egyik rendszertől a másikig vezető útvonal több lehetséges utat is követhet. Ezeket érdemes megvizsgálni. Erre az egyik legjobb program traceroute. A lassabb kapcsolatok esetén értékes információkhoz jutunk, amit figyelembe véve hatékonyabb útvonalat kereshetünk.

ASS letapogató

ASS egy rendszer letapogató. Támogatja a következő protokollokat: IRDP, IGRP, EIGRP, RIPv1, RIPv2, CDP, HSRP és OSPF. Opciói: pasziv mód (./ass -i eth0), aktiv mód (./ass -i eth0-A)

Protos protocol scanner

Normal Windows kiszolgáló ellenőrzése során: Windows letapogatása alatt lehet futtatni ICMP IGMP TCP UDP módokba. Támogatja cisco router módot is: Cisco alatt lehet futtatni ICMP IPenc TCP IGP UDP GRE SWIPE MOBILE SUN-ND EIGRP

DMitry

A DMitry (Deepmagic Information Gathering Tool) egy információ gyûjtõ eszköz. Megkeresi internet whois adatokat. Megkeresi system és server adatait. Megkeresi a SubDomain és host adatokat. Megkeresi E-Mail adatokat. Végre hajt egy a TCP Portscan -t.

DNS-Ptr

A DNS-Ptr megszerzi DNS és Ip információkat.

Goog Mail Enum

Google közreműködésével felsorolja megtalált email címeket a kért szerverről.

Dig

Dig (domain information groper) információkeresgélő. Olyan rugalmas eszköz, amivel letapogatható a DNS name server.

Netenum

Netenum, egy egyszerű ping eszköz. Megtudjuk a host IP címét és, hogy működik-e.

SMTP-Vrfy

SMTP Protocol Hacker eszköz. SMTP-Vrfy megvizsgálja users/mail bejegyzést egy fáj tartalma alapján (names.txt).

Penetration Eszközök

MsfCli MsfConsole

Exploit támadásra használható program. Parancs beállítása után exploit támadás. MsfConsole utasítás kiadása után a konzolba írjuk be: msf>help, ez kiírja a beállítást. Show exploits (kiírja exploit listát), show payloads (támadási mód kiválasztása)

Maintaining Access Eszközök

HttpTunnel Client

Perl és php nyelven íródott és ingyenes program. Windows és linux rendszeren is használható. Elsősorban tűzfal mögött dolgozók érdeklődésére számíthat a HttpTunnel program, mivel segítségével az internet olyan szolgáltatásait (telnet, ftp) is igénybe lehet venni, amelyek nem minden esetben elérhetőek a tűzfal mögött. Az alkalmazás a tűzfal által átengedett http protokoll felhasználásával kétirányú virtuális kapcsolatot létesít más kiszolgálókkal, és így lehetőség nyújt más protokollok használatára is. HttpTunnel client program természetesen a server részével HttpTunnel Server programmal használható.

HttpTunnel Server

Elsősorban tűzfal mögött dolgozók érdeklődésére számíthat a HttpTunnel program, mivel segítségével az internet olyan szolgáltatásait (telnet, ftp) is igénybe lehet venni, amelyek nem minden esetben elérhetőek a tűzfal mögött. Az alkalmazás a tűzfal által átengedett http protokoll felhasználásával kétirányú virtuális kapcsolatot létesít más kiszolgálókkal, és így lehetőség nyújt más protokollok használatára is. HttpTunnel Server program természetesen a kliens részével HttpTunnel Client programmal használható.

Tinyproxy

A tinyproxy, ami egy pehelysúlyú HTTP proxy. Tartalmat szűrni nagyon kevés proxy tud. TinyProxy viszont igen.

Privoxy

Ez egy proxy, amit be lehet állítani bármelyik böngészőnek. Átnézi az oldal forrását, és kicsit megváltoztatja (kiszedi a reklámot). A privoxy csomag a címlekérdezést (DNS) teszi fölöslegessé, tehát a címlekérdező címének megállapítását teszi lehetetlenné.

CryptCat

Cryptcat netcat továbbfejlesztett változata. Titkosított adat átküldésre képes. Használható Windows NT, BSD and Linux rendszeren. Cryptcat gyakorlatilag nullára csökkenti az adatok megváltozásának veszélyét. Cryptcat olyan Unix eszköz, ami képes olvasni, és írni adatokat hálózati kapcsolat során.

Privilege Escalation Eszközök

EtterCap

Hálózat vizsgálatára, lehallgatására használható. Rengeteg információt lehet gyűjteni. Grafikus felületen könnyen használható, igen sokat tanulhatunk a segítségével a hálózat működéséről. Ilyeneket, mint host típusa, operációs rendszer, használt port a kapcsolat során, milyen szerver stb.

Wireshark

Az Ethereal új néven folytatja életét Wireshark (Drótcápa). Hálózat vizsgálatára, lehallgatására használható. Rengeteg információt lehet gyűjteni. Grafikus felületen könnyen használható, igen sokat tanulhatunk a segítségével a hálózat működéséről.

EtherApe

Grafikus felületen követjük figyelemmel a csomagok útját a hálózaton. Kérhetjük ip vagy ethernet vagy tcp alapján a csomag megfigyelést. Folyamatos figyelésével a támadok is észlelhetők kapcsolódás alapján.

Network Mapping

Hálózati adatgyűjtés. Ezekkel a programokkal hálózattal kapcsolatos információk gyűjthetők.

Netdiscover felderítő

Netdiscover egy active/passive felderítő eszköz. Főként alkalmas wireless hálózatokhoz. Kitűnő segédeszköze wardrivingnek. Használható hub/switched hálózatokhoz.

Hping

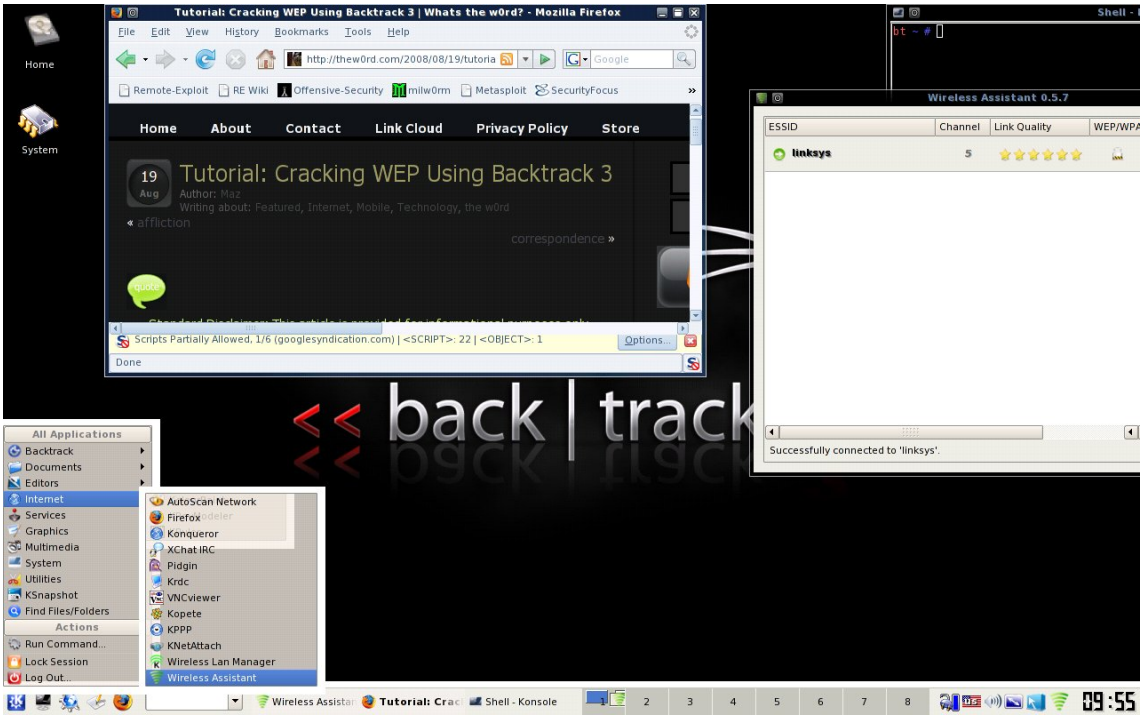
Nagy tudású pingelő, és csomaggeneráló eszköz. Küldhető csomagok fajtái: TCP, UDP, ICMP.

Trivial File Transfer Protocol (TFTP)

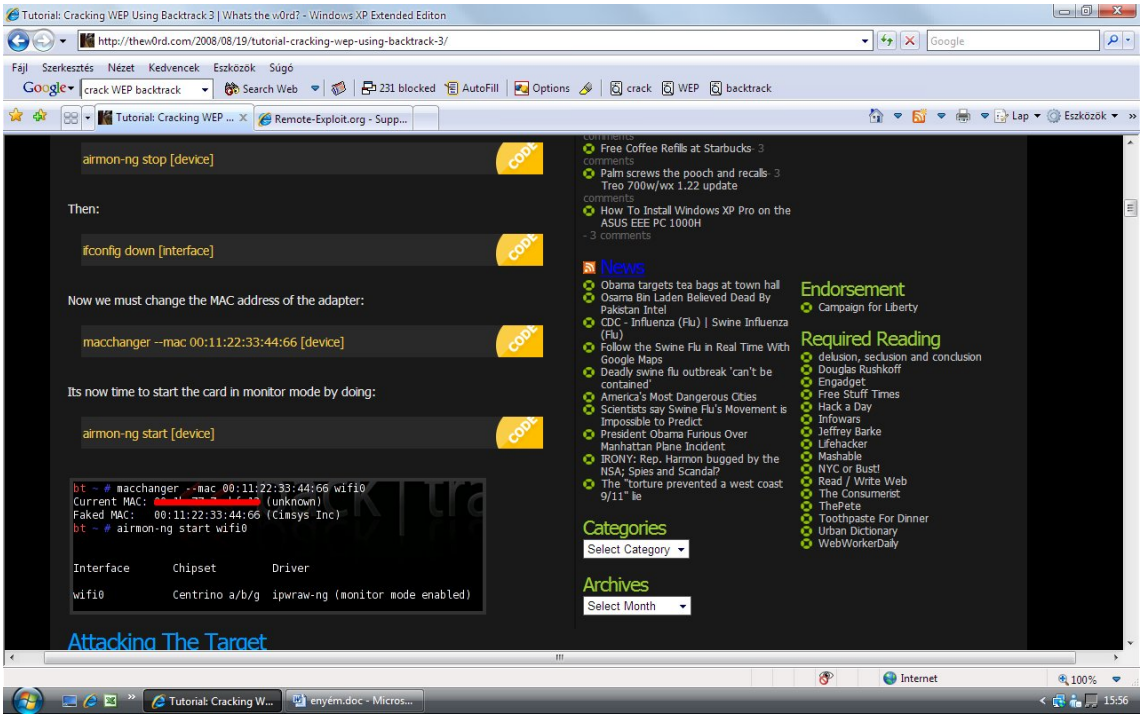
TFTP gyorsabb, mint az FTP. Ennek oka, hogy nem TCP, hanem UDP (User Datagram Protocol) protokollon működik. Az UDP gyorsabb fájlátvitelt tesz lehetővé a hálózaton, de kevésbé biztonságos.

Nmap

Nmap elkészítésének szándéka az volt, hogy lehetőséget biztosítson a rendszeradminisztrátoroknak és a kíváncsi személyeknek, hogy letapogathassanak nagy hálózatokat és megállapíthassák, mely hostok működnek és milyen szolgáltatásokat kínálnak.



A Backtrack segítségével, a legtöbb 64 és 128 bites WEP titkosítással védett, hozzáférési pont feltörhető. Tehát a lényeg, hogy egy olyan hozzáférési ponthoz szeretnénk csatlakozni, amely jelszóval védett, de mi nem tudjuk a jelszót. Ezt a problémát tehát, könnyen megoldhatjuk. Szükséges a terv végrehajtásához, a Backtrack cd-n vagy USB –n, 802.11 kompatibilis hálózati kártya, és persze a vezeték nélküli hozzáférési pont, vagy router, amely WEP titkosítással védett. A Backtrack 3 beszerezhető, a http://www.remote-exploit.org/backtrack_download.html címről, cd image, usb, illetve VMware verzióban. Telepítése is konfigurálása után, ha felismerte a hálózati kártyánkat, akkor kezdődhet a WEP törés folyamata, mely lépésről lépésre le van írva, a http://thew0rd.com/2008/08/19/tutorial-cracking-wep-using-backtrack-3/ címen.



Köszönetnyilvánítás

Köszönetem kifejezése révén szeretném ebben a pár sorban, megemlíteni Dr. Krausz Tamás témavezetőm segítő munkáját, mely a szakdolgozat megírására vonatkozó javaslatait,tanácsait és a segédanyagok rendelkezésemre bocsátását foglalta magában.

Összefoglalás

Napjainkban egyre inkább elterjednek a vezeték nélküli hálózatok az átlag felhasználók köreiben, épp úgy, mint a vállalatoknál, cégeknél. Ezt a tényt köszönhetjük akár a teljesítmények jelentős növekedésének, vagy az árak drasztikus csökkenésének, illetve az eszközök könnyű telepítésének és az emberek kényelmi elvárásainak. Lényegesen kényelmesebb érzetet érhetünk el például, ha csak arra gondolunk, hogy egy otthoni hálózatban a ház több pontjáról, vagy akár a teraszon ülve is kihasználhatjuk lehetőségeinket. A másik példa, vegyünk egy vállalatot, ahol már kiépített hálózat van, bővítésre lenne szükség, de a kábelezés rengetek munkával, és persze mindenütt vezetékkötegekkel járna, illetve a mobilitást sem egyszerű megoldani. Ekkor egy jól konfigurált vezeték nélküli hálózat lehet a megoldás. A rendelkezésre álló eszközöknek azonban teljes mértékben meg kell felelniük a biztonsági elvárásoknak, szerencsére a gyártók egyre nagyobb és nagyobb átviteli sebességre képes technológiával felszerelt és a mai biztonsági normáknak megfelelő termékeket dobnak a piacra. A sebezhetőség főként a nagyobb hálózatok esetén elfogadhatatlan, de nem lehet elégszer felhívni a figyelmet, hogy a veszély a kis vállalatok és az otthoni hálózatok tulajdonosait is fenyegeti. Itt főleg azon veszélyekre gondolok, mint személyazonossággal való visszaélés, vagy a hálózat üzemeltetője nevében bűncselekményt követ el. Ebből gondolom, mindenki levonja a következtetést, hogy bizony érdekében áll gondoskodni a megfelelő védelemről. A vezeték nélküli hálózat kiépítésénél, mikor megvásároljuk telepítendő eszközöket, ne csak a átviteli sebesség felső határát és az árat vegyük figyelembe! Győződjünk meg róla, hogy a 802.11x alszabványai által támogatott biztonsági szabványai közül, melyeket támogatja az eszközünk. A mai középkategóriás AP-k közül már mindegyikben van WEP, WPA és WPA2 protokollok is megtalálható. Vásárlás után, ezeket az eszközöket megfelelően telepítenünk is kell, mivel a gyártók által forgalmazott eszközök eredetileg nyílt hálózati beállításokkal rendelkeznek. Konfigurálásкor minimum a WPA biztonsági protokoll beállítása javasolt, mivel a WEP rendelkezik hiányosságokkal a biztonság terén, ezért ha csak lehet, ne ezt válasszuk a hálózat védelmére.

Irodalom jegyzék:

Internet:

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

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

www.pcexpert.hu

http://thew0rd.com/2008/08/19/tutorial-cracking-wep-using-backtrack-3/

http://www.remote-exploit.org/backtrack.html

http://blacklinux.uw.hu/html/backtrack.html

http://blacklinux.uw.hu/html/backtrack2.html

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

http://www.cisco.com/web/HU/solutions/smb/products/wireless/wireless_primer.html

http://www.pdacafe.hu/blog/vezetek-nelkul-wireless-es-wifi.html

http://www.w-lantech.hu/index.php?file=content-wlan

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

http://www.technet.hu/pdamania/20051107/vezetek_nelkuli_halozat_otthon_-_ii_resz/

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

Egyéb forrás:

Matthew Gast - 802.11 Wireless Networks The Definitive Guide Oreilly Excellent (2002)

CISCO SYSTEMS Panem Könyvkiadó – Jim Geier - Vezeték nélküli hálózatok

Wireless Networks First Step (2005)

AirDefense White Paper Wireless LAN Security - What Hackers Know That You Don’t (2003)

Andrew S. Tanenbaum - Számítógépes hálózatok – Panem könyvkiadó

Eric Geier - Wi-Fi Hotspots –Cisco Press

Krasznay Csaba - Vezeték nélküli hálózatok biztonsága –kancellar.hu