Debreceni Egyetem

Informatikai Kar

Vezeték nélküli hálózatok biztonsági kérdései

Témavezető:

Dr. Krausz Tamás

egyetemi adjunktus

Készítette:

Miholics László

mérnök informatikus

Debrecen

2011

Tartalomjegyzék

1. Bevezetés

A dolgozatom kiválasztásakor próbáltam arra törekedni, hogy egy olyan témát válasszak, mellyel a későbbiek folyamán is szeretnék majd foglalkozni. Mióta informatikát tanulok, azóta érdekelnek a hálózatok, és azon belül a vezeték nélküli hálózatok. Napjainkban az infokommunikációs hálózatokat egyre inkább a sokszínűség jellemzi. A mai világban egyre több és több információ áramlik az internetes szuper sztrádán, így a felhasználók igényei is egyre nagyobbak; az emberek adatátviteli szükségleteinek kiszolgálására ma már rengetek különböző technológia és átviteli közeg áll rendelkezésre, ilyen például a koaxiális kábel, rézpár, üvegszálas kábel és a szabad tér.

Az információáramlás alapvetően egy adó és egy vevő között zajlik egy csatorna segítségével, amelyben az üzenetek vándorolnak. A vezeték nélküli hálózatoknál is megjelenik az információáramlás e formája, az adónak és vevőnek a hálózathoz tartozó eszközök felelnek meg, például egy mobiltelefon és egy router a csatornának pedig a levegő. A számítógépes hálózatoknál már nem számít újdonságnak a vezeték nélküliség, már 10-15 éve jelen van ez a technológia. Hiába hogy már régóta van jelen ez a módszer a számítógépes hálózatokban, és igen gyorsan fejlődik, nagyon lemaradt a biztonság terén a vezetékes hálózatok biztonságától. Ahogy egyre jobban belemélyedtem a dolgozatom témájába, rájöttem, hogy igazából nagyon sok esetben a vezeték nélküli hálózatoknál igen egyszerűen meglehetne teremteni a megfelelő biztonságot. Nagyon sok esetben maguk az emberek nem tudják, illetve nem akarják ráfordítani a kellő időt és energiát arra, hogy megakadályozzák, illetéktelen felhasználók bejutását privát hálózatokra. Erre azt az egyszerű példát tudom felhozni, hogy egy neves mobiltelefonos portál munkatársai 2007-ben mikor már nagyon elterjedt volt a vezeték nélküli hálózat, végigmentek több Magyarországi nagyvároson és nézték az utcáról, hogy mely hálózatokra lehet egyszerűen felcsatlakozni. Elkészítettek egy felérést, miszerint nagyon rossz eredmények születtek. Ezt a cikküket én is olvastam, és akkoriban már nagyon foglalkoztatott ez a témakör, és ezért is választottam ezt dolgozati témának.

A dolgozatom elején általánosan ismertetem a vezetékes és vezeték nélküli hálózatokat, azok különbözőségeit. Ezt követően bemutatom a vezeték nélküli hálózatok fajtáit, az adatátviteli szabványokat, majd egy WiFi-s hálózat létrehozásának lépéseit. A következő részben a vezeték nélküli informatikai hálózatok biztonságáról lesz szó, ezt majd részletesebben is taglalom. A szakdolgozatom végén pedig egy példán keresztül mutatom be, egy vezeték nélküli hálózat feltörését.

Szakdolgozatom egyik célja, hogy ezt az érdekes témát, mindenki számára érthetően tárjam az olvasó elé.

2. A vezetékes és vezeték nélküli hálózatok különbségei, jellemzői

A vezetékes hálózat kialakítása, manapság már kevésbé elterjedt, vagy legalábbis visszaszorulóban van. A vezeték nélküli technológiák a számítógépes értelemben lassan teljesen kiszorítják a kábeleket az otthonokból, intézményekből, gyárakból. Pedig néha valóban szükséges ilyen felépítésű rendszer kialakítása a háztartásokban is. Abban az esetben, ha nem kell nagy távolságra megosztani az Internetet, például egyetlen helyiségben (dolgozószoba, iroda) két-három számítógép között, vagy ahol nem számít az asztal mögé rejtve hány kábel fut, akkor érdemes ilyen jellegű hálózatot kialakítani. A vezeték nélküli hálózatok ezzel szemben gyors és kényelmes megoldást jelentenek, csupán felkapcsolódunk a hálózatra és rögtön bárhonnan használhatjuk a hatókörön belül nem vezetékes kapcsolat létesítésére alkalmas eszközeinket. Mindkét hálózattípusnak vannak előnyei és hátrányai, azt kell eldönteni, mi felel meg jobban az ember igényinek.

A vezetékes hálózatokat jellemzi, hogy általában gyorsabban lehet dolgozni, játszani és internetezni rajtuk keresztül. Ezek működése rendkívül stabil, csak a vezeték fizikai sérülése esetén válik működésképtelenné. Biztonságosak, a rajta átmenő forgalmat gyakorlatilag nem

lehet megfigyelni. A gépek közötti több száz métert meghaladó távolság esetén is stabil és gyors kapcsolat építhető ki. A vezetékes hálózathoz kapcsolódó eszközök olcsóbbak a vezeték nélkülieknél.

A vezeték nélküli hálózatok jellemzői, hogy egyszerű az infokommunikációs hálózat kialakítása akár több eszköz között is. Azokat a nem vezetékes eszközöket tekintve, amelyekkel csatlakozunk a hálózatokra, sokkal nagyobb a mozgási szabadság, mert mozoghatunk az eszközökkel, anélkül, hogy beleakadnánk kábelekbe. A vezeték nélküli hálózatok sokkal rugalmasabbak, bővíthetőbbek, mint a vezetékes hálózatok.

2.1 Mi az a WiFi/ WLAN?

A WLAN az angol Wireless Local Area Network szó rövidítése, melynek jelentése vezeték nélküli helyi hálózat, amire legtöbbször a „vezeték nélküli hálózat”, WiFi vagy WLAN nevet használják. A WiFi működése hasonló a LAN hálózatokéhoz, csak a jelek más közegben terjednek. Míg a LAN vezetéket használ (hálózati kábel), addig a WiFi a levegőben továbbítja az információt.

Azért előnyös a WiFi, mert teljes szabadságot, és így mobilitást biztosít. Nem leszünk helyhez kötve számítógépünkkel, így Internetezhetünk a folyosóról, az irodánkból, de akár még az udvarról is.

3. A vezeték nélküli hálózatok

3.1 A vezeték nélküli hálózatok története

- ***1942*** – Feltalálják és szabadalmaztatják a frekvencia-ugrásos rádiótitkosító technikát, melyet később „szórt-spektrumú” technikának neveztek. Ez a feltalálás George Antheil zeneszerző és Hedy Lamarr színésznő nevéhez fűződik. Később az amerikai tengerészetnek adják át, akik a II. Világháborúban még nem találták használhatónak.
- ***1958*** – A korábban átvett technikát az amerikai tengerészet tovább fejlesztette és így létrehozták az első rádiós kommunikációs chipet.

- ***1985*** – Az amerikai tengerészet az 1985-ben kifejlesztett technológiát elérhetővé teszi az emberek számára.

- ***1989*** – Az Amerikai Hírközlési Hatóság (FCC - Federal Communications Commission) három szabad rádió sávot engedélyez a technológiának

- ***1990*** – Az IEEE (Institute of Electrical and Electronics Engineers) megkezdi a vezeték nélküli kapcsolat szabványának kidolgozását az Ipari, Tudományos és Orvosi (ISM - Industrial, Scientific and Medical) spektrumban.

- ***1997*** – Az FCC engedélyezi, hogy használjanak egy negyedik frekvencia sávot is. Az IEEE elfogadja a 802.11 "over-the-air" vezeték nélküli kliensek és alap-állomások közötti interfészt, amely még nem garantálta a szabványok együttműködését.

- ***1999*** – Megalakul a Vezeték Nélküli Ethernet Kompatibilitás Szervezet (WECA - Wireless Ethernet Compatibility Alliance) a 802.11 szabványban való együttműködés összehangolására. Még ebben az évben az IEEE elfogadja a 802.11b és 802.11a szabványt.

- ***2000*** – A WECA megkezdte WiFi hitelesítő programját a 802.11b szabványt támogató termékekre. Ebben az évben a Microsoft kiadja a Windows 2000 –ret WLAN sniffer funkcióval kiegészítve. A Carlson Hotels Worldwide (a Country Inns & Suites, a Radisson Hotels és a Regent International Hotels tulajdonosa) bejelenti vezeték nélküli szolgáltatását.

- ***2001*** – A Starbucks vezeték nélküli hotspot szolgáltatását elindítja. Bejelentik a Vezetékessel Egyenértékű Titkosítás-t (WEP - Wired Equivalent Privacy), miszerint a 802.11 biztonsági megoldása bizonyítottan megbízhatatlannak minősült. Scott Fluhrer, Itsik Mantin, és Adi Shamir kutatók nevéhez fűződik. A WEP bejelentését Scott Fluhrer, Itsik Mantin, és Adi Shamir kutatók tették. Még ebben az évben jelennek meg 802.11a szabványú termékek a piacon.

- ***2002*** – A Lucent Technologies bemutatja, hogy a felhasználók hogyan képesek váltani úgy WiFi és 3G mobil hálózatok között, hogy az internet kapcsolatuk megszakadna. A WECA új szervezetté alakul, WiFi Alliance (WFA, WiFi szövetség) néven, elindítja a

802.11a hitelesítő tesztjeit illetve bejelenti a WPA (WiFi Protected Access, WiFi védett hozzáférés) biztonsági módszert a WEP leváltására.

- ***2003*** – A WFA elindítja WiFi ZONE programját publikus hotspotok hitelesítésére. Az Intel bemutatja a Centrino technológiát, amely hardveresen támogatja a vezeték nélküli kapcsolatokat. Megjelentek az első, még nem véglegesített 802.11g szabványt támogató termékek. A WFA hitelesíttette az első WPA-t támogató termékeket. Ekkor már több mint 40 millió 802.11 szabványt támogató terméket adtak el világszerte, illetve megjelentek az első 802.11a és 802.11g szabványt egyszerre támogató termékek is. A Verzion 150 darab olyan telefonfülkét telepített ami WiFi-re képes. Az IEEE engedélyezte a végleges 802.11g szabványt. Ekkora már 112 cég 865 terméke kapta meg a hivatalos WiFi hitelesítést 2000 óta. A WPA támogatását kötelezővé tették a WiFi hitelesítés folyamatában.

- ***2008*** – A 802.11y szabvány megjelenése.

- ***2009*** – Az IEEE engedélyezi a 802.11n szabványt, amely sebessége és hatótávolsága nőtt. A 802.11n szabvány természetesen kompatibilis 802.11a/b/g szabványokkal, de ha két 802.11n berendezést kapcsolunk össze, akkor akár 12-szer gyorsabb eredményt kaphatunk a 802.11g szabványhoz képest.

- ***2011*** – Manapság már rengeteg WiFi-s termék van, saját megfigyeléseim alapján az egyik húzóágazattá a mobiltelefonok és a táblagépek váltak, manapság már majdnem mindegyik frissen kiadott elektronikai készülékben találhat WiFi. Magyarországon is lassacskán, de biztosan látszik a vezeték nélküli hálózatok térnyerése, távolsági buszokon, éttermekben, közintézményekben.

3.2 Vezeték nélküli hálózatok típusai

3.2.1 Vezeték nélküli hálózati topológiák

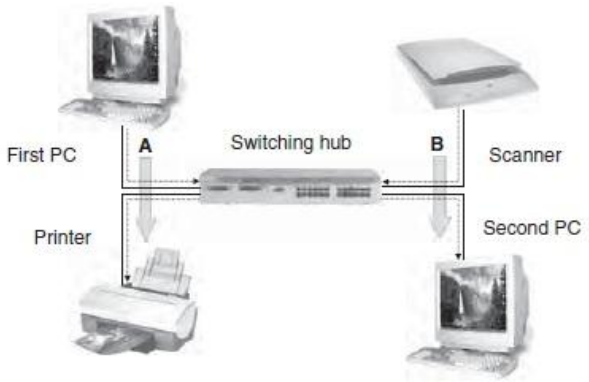
Pont-Pont kapcsolat[1]

A vezeték nélküli topológiák közé tartozik például a Pont-Pont kapcsolat. Pont-pont kapcsolat. Rendszerint a nagy távolságú, valamint az egyes routerek közötti összeköttetések ilyenek. Pont-pont összeköttetésekből felépülő nagyobb hálózat struktúrája lehet: csillag, gyűrű, fa, teljes, vagy szabálytalan. A magyarországi akadémiai hálózat (HBONE) budapesti magja gyűrű, a vidéki részek pedig faág-szerűen kapcsolódnak. A Budapesti egyetemi hálózatok szintén gyűrűk, ezek több ponton is kapcsolódnak a HBONE-hoz. A Pécsi Universitas hálózata (UPNET) fa, de tervezzük gyűrű kialakítását is. A gyűrű topológia a működési biztonságot növeli. A fastruktúra előnye a hostok (alhálózatok) közötti minimális routerszám, hátrány a forgalom torlódása. A teljes összeköttetésű hálózat mindkét előnnyel rendelkezik, azonban rendkívül drága. A pont-pont kapcsolatokból felépülő hálózatoknál még megemlíteném a store-and-forward és a packet switch fogalmat.

Store-and-forward: A csomag a routerben tárolásra kerül, amíg a következő adatvonalon lehetségessé nem válik a továbbítás

Packet switch: Az adatcsomag tartalmazza a célállomás címét, ennek alapján a router csak a megfelelő adatvonalon továbbítja a csomagot.

*Pont-Pont kapcsolat látható a **1**. ábra*[2]



[1] Wireless Security - The Newnes Know It All Series (2009), 49. old.

[2] Wireless Security - The Newnes Know It All Series (2009), 50. old.

Láthatjuk, hogy ez a topológia sokban hasonlít egy vezetékes topológiára, de nagyon sok esetben alkalmazzák vezeték nélküli megoldásoknál.

Ilyen alkalmazási területek például:

- p2p vagy ad-hoc WiFi kapcsolat
- vezeték nélküli MAN visszacsatolás figyelő
- Lan vezeték nélküli áthidaló
- Bluetooth
- IrDa

Csillag topológia vezeték nélküli hálózatoknál[3]

A számítógépek, WiFi-es eszközök egyazon csomópontra csatlakoznak. Ez a csomópont például egy router. Előnye: vonalszakadás esetén csak az adott eszköz válik le a hálózatról. Hátránya: a szerver túlterheltté válhat. A vezeték nélküli hálóatok csomópontja függetlenül attól, hogy az egy WiMAX bázisállomás, WiFi hozzáférési pont, Bluetooth Master eszköz vagy egy ZigBee PAN koordinátor, hasonló szerepet töltenek be mint egy hub a vezetékes hálózatban.

Csillag topológia középen egy WiFi hozzáférési ponttal 2. ábra[4]

[3] Wireless Security - The Newnes Know It All Series (2009), 50. old.

[4] Wireless Security - The Newnes Know It All Series (2009), 51. old.

Mesh hálózatok[5]

A vezeték nélküli IEEE 802.11 szabvány egy Mesh szerkezettel lett kiegészítve. A 802.11s szabvány célja egy olyan protokoll létrehozása, mely önállóan tudja konfigurálni az útvonalakat az elérési pontok között egy "mindenki mindenkivel" felépítésben. Az ilyen hálózat alapelve az elérési pontok olyan széthelyezése és egy hálózattá kapcsolása, hogy mindegyik csomópontja kapcsolatot tudjon létesíteni a szomszédos pontokkal. Csak a végső kapcsolóelemet kell egy állandó hálózatra, pl. az Internetre kötni. A Mesh hálózat felépítése egy decentralizált hálózaton alapul, relatíve olcsó és a legfontosabb előnye a megbízhatóság. A hálózat mindegyik csomópontja több szomszédos pontból és pontba vehet, illetve küldhet át üzeneteket. Ezért, ha az egyik csomópont kapcsolása megszűnik, a hálózat automatikusan újabb utat keres az adatok továbbítása számára. A standard WDS módtól eltérően a Mesh routerek automatikusan azonosítják szomszédjaikat és tanulják ki a legegyszerűbb elérhetési útvonalakat. Nem kell ezért manuálisan konfigurálni az elérési pontokat. A rendszer e bizonyos fokú "önirányítása" csökkenti a rendszerbővítési költségeket. A Mesh hálózat felépítését rugalmasság, biztonság és integritás jellemzi. Azonban a megfelelő hivatalos szabvány hiányában a különböző gyártók elérési pontjai nem biztos, hogy kompatibilisek lennének egymással. Az IEEE 802.11s szabvány megteremtése ezt a helyzetet hivatott elkerülni.

3.2.2 WPAN – „személyes vezeték nélküli hálózat”[6]

A Wireless Personal Area Networks kifejezés rövidítése. Ennek a technológiának segítségével a felhasználók személyes környezetükben (POS) használt eszközei (pl. személyi digitális asszisztensek, mobiltelefonok és laptopok) ad hoc vezeték nélküli kommunikációra képesek. A POS betűszó a személy legfeljebb 10 méteres környezetét jelöli. Jelenleg a Bluetooth és az infravörös fény a WPAN két legfontosabb technológiája. A Bluetooth egy kábelhelyettesítő technológia, ami rádióhullámokat használ legfeljebb 10 méteres távolságban történő adatátvitelre. A Bluetooth adatok falon, zseben és aktatáskán keresztül is átvihetők. A Bluetooth technológia fejlesztését a Bluetooth SIG (Special Interest Group) végzi, ami 1999-ben adta közre a Bluetooth 1.0-s verziójának specifikációját.

[5] Wireless Security - The Newnes Know It All Series (2009), 52-54. old.

[6]Chris Hurley és tsi (szerk) How to Cheat at Securing a Wireless Network, Syngress Publishing (2006)

Nagyon kis távolságra (1 méter vagy kevesebb) lévő eszközök összekötésének másik módja az infravörös kapcsolat létrehozása.
A WPAN technológiák fejlesztésének szabványosítására az IEEE megalkotta a 802.15 munkacsoportot. Ez a munkacsoport fejleszti a WPAN szabványt a Bluetooth 1.0-s verziójú specifikációja alapján. A szabványtervezet elsődleges célkitűzése a kis komplexitás, a kis áramfelvétel, az együttműködési képesség és a 802.11 hálózatokkal való együttélés.

3.2.3 WLAN – „helyi vezeték nélküli hálózat”[7]

A Wireless Local Area Networks kifejezés rövidítése. Ennek a technológiának a segítségével a felhasználók vezeték nélkül köthetők össze helyi hálózatban (például egy vállalati vagy egyetemi épületben vagy egy nyilvános helyen, például repülőtéren). A WLAN ideiglenes irodákban vagy más helyeken használhatóak, ahol kiterjedt kábelezés nem oldható meg, vagy egy meglévő LAN-t kell kiegészíteni, hogy a felhasználók különböző időpontokban különböző helyeken dolgozhassanak egy épületben. A WLAN-ok kétféleképpen működhetnek. Az infrastrukturális WLAN-okban a vezeték nélküli állomások (rádiós hálózati kártyával vagy külső modemmel rendelkező eszközök) vezeték nélküli hálózatelérési pontokhoz csatlakoznak, melyek hidakként működnek az állomások és a meglévő gerinchálózat között. Az egyenrangú (ad hoc) WLAN-okban kis helyen (pl. egy konferenciateremben) számos felhasználó képes ideiglenes hálózatot kialakítani hozzáférési pontok nélkül, ha nincs szükségük hálózati erőforrásokra.
1997-ben az IEEE elfogadta a WLAN-okra vonatkozó 802.11 szabványt, amely 1 és 2 Megabit/másodperc (Mbit/s) közötti átviteli sebességet határoz meg. A 802.11b, amely egyre inkább domináns helyzetre tesz szert a szabványok között, 11 Mbit/s sebességet tesz lehetővé 2,4 gigahertzes (GHz) frekvenciasávban. Egy másik új szabvány a 802.11a, amely 54 Mbit/s maximális adatátviteli sebességet tesz lehetővé 5 GHz-es frekvenciasávban.
WPAN-ok (vezeték nélküli személyes hálózatok)

[7] Chris Hurley és tsi (szerk) How to Cheat at Securing a Wireless Network, Syngress Publishing (2006)

3.2.4 WMAN – „városi vezeték nélküli hálózat”[8]

A Wireless Metropolitan Area Networks kifejezés rövidítése. Ez a technológia lehetővé teszi egy nagyváros különböző pontjai közötti vezeték nélküli kapcsolatokat (például több irodaház között egy városban vagy egy egyetem területén) az optikai kábel vagy rézvezeték, valamint a bérelt vonalak magas költsége nélkül. A WMAN hálózatok ezen kívül tartalékrendszerként szolgálhatnak vezetékes hálózatok mellett, ha a vezetékes hálózatok elsődleges bérelt vonalai használhatatlanná válnak. A WMAN hálózatok rádióhullámokat vagy infravörös fényt használnak adatátvitelre. Egyre keresettebbek a szélessávú vezeték nélküli hálózatok, melyek nagy sebességű Internet hozzáférést biztosítanak. Bár különböző technológiák léteznek, például az MMDS (multichannel multipoint distribution service, többcsatornás többpontos elosztó szolgáltatás) és az LMDS (local multipoint distribution services, helyi többpontos elosztó szolgáltatás), az IEEE 802.16 szélessávú vezeték nélküli hozzáférési szabványokon dolgozó munkacsoportja még mindig fejleszti ezeknek a technológiáknak a szabványait.

3.2.5 WWAN – „országok közötti vezeték nélküli hálózat”[9]

A Wireless Wide Area Networks kifejezés rövidítése. Ez a technológia Internetelérést biztosít egy adótorony és cellahálózaton keresztül. Tulajdonképpen a mobilszolgáltatók adatkommunikációs szolgáltatása, mely lehet GPRS alapú, vagy valamilyen második, harmadig generációs hálózaton üzemelő csomagkapcsolt adatszolgáltatás. Rendszerint okos telefonok, táblagépek és PDA-k használják ezt a mobilhálózaton keresztüli Internet elérést, azonban napjainkban egyre több laptopban is előfordul WWAN egység. Nagy előnye, hogy szinte mindenhol biztosítja az internet elérést, sebessége egyelőre azonban mérsékelt.

[8] Wireless Security - The Newnes Know It All Series (2009)

[9] http://www.scribd.com/doc/38236010/1-szemeszter

4 Vezeték nélküli adatátviteli szabványok

4.1 IrDA[10]

Ma már nem kerül a piacra olyan telefon, amelyikben infravörös port lenne. Pedig pár éve még igencsak fontos volt, hiszen a Bluetooth előtt ez volt az egyetlen vezeték nélküli adatátviteli módszer telefonok és bármilyen más eszközökben. Az infra azonban lassú (bár léteznek az óta gyorsabb szabványok), a mobiltelefonokban maximum 115,2 kbps sebességű lehetett, de ez is ritka volt. Ráadásul az infra hatótávolsága 30 centiméter körül alakult mobil eszközöknél, plusz kellett a vizuális kontaktus is a két berendezés között. Az infraport a fentiek miatt a Bluetooth terjedésével egyre inkább kiszorult a telefonokból. A GPRS sebességét még át tudta vinni adott esetben egy számítógépre, de a 3G esetén már lehetetlen volt ez. Pedig néhány éve még infrán küldtünk egymásnak telefonkönyv bejegyzéseket, bizonyos Nokia készüléknél pedig a Snake játszható volt két telefonnal is, egymás ellen.

Az ***IrDA DATA***.Ez az ága az IrDA szabványnak a régebbi, ez szolgál tényleges adatátvitelre 9,6 kbit/sec-től egészen 4 Mbit/sec-ig. Az IrDA átvitel 1 méter távolságig kell, hogy működjön (létezik alacsony fogyasztású változat is, ahol ez csak 20 cm), kétirányú adatkapcsolatot biztosít, és CRC kódolással védi az adatokat. A fizikai rétegre az IrLAP (Link Access Protocoll) épít, ami biztosítja a hibajavítást, valamint a környezetben lévő készülékek felismerését. A következő réteg az IrLMP (Link Management Protocoll) ami biztosítja, hogy egy fizikai IrDA kapcsolaton keresztül több logikai kapcsolat is működhessen, illetve lehetőséget biztosít, hogy a partnerek megvalósított protokolljait és szolgáltatásait feltérképezzük. Ez a 3 (fizikai, IrLAP, IrLMP) rétegkötelező, a további protokollok már opcionálisak. A 4. rétegben IAS (Information Access Service) információt nyújt a megvalósított protokollokról, míg a Tiny TP (Transfer Protokol) az adatok átvitelét szabályozza, szükség szerint felszabdalva és összerakva az átviendő adatmennyiséget. Az 5. rétegben találhatóak a leglényegesebb protokollok, alapjában véve ezek határozzák meg, az elérhető szolgáltatásokat.

- ***IrCOMM*:** soros és párhuzamos port emuláció (ezt használják az IrDA-t támogató mobiltelefonok)

[10] http://en.wikipedia.org/wiki/Infrared_Data_Association

- ***IrOBEX*:** objektumokat (fájlokat) lehet cserélni vele, például a Palm sorozat gépei a névjegyek infravörös cseréjekor egy vCard típusú fájlt küldenek át IrOBEX szabvány szerint.

- ***IrTran*-P:** képek elküldéséhez, ezt támogatják például a Casio digitális fényképezőgépei és a Nokia 9110 és a Sharp WinCE palmtopjai.

- ***IrMC*:** mobil telefonok kezelése, a telefonkönyv, a telefonban lévő naptár, hívás vezérlés és magának a hangnak az átvitelét specifikálja.

- ***IrLAN*:** LAN hozzáférés IrDA-n keresztül.

Kicsit kilóg a sorból az ***IrDA Lite***, ami egyszerűbb eszközöknek egy olyan megvalósítási lehetőséget kínál, ami kompatibilis a teljes IrDA protokoll csomaggal, de egyszerűbben megvalósítható. A gyakorlati tapasztalat eddig azt mutatta, hogy a Palm sorozat mind az IrCOMM mind pedig az IrOBEX-et jól kezeli, míg a WindowsCE az IrCOMM-ot tudja viszont a fájlmásoláshoz valami speciális Microsoftos protokollt használ. Az infrás mobiltelefonok közül a Nokia 6110 kivételével mindegyik jól kezeli az IrCOMM és az IrOBEX protokollokat. A 6110 valószínűleg az IrLMP vagy az Tiny TP-ra épített egy saját protokollt, ami miatt Palm topokkal külön szoftver nélkül nem használható. A szabványos készülékeknél viszont nagyon látványos, ahogy például a Siemens S25 telefonon kikeresünk valakit a telefonkönyvből, a menüből kiválasztjuk az elküldését infrán és a Palm-ra egy pillanat múlva megérkezik a név a telefonszámmal, és azonnal bekerül a névjegyek közé.

Az ***IrDA control*** nagyobb hatótávolságú, de lassabb berendezésekhez készült, tipikusan billentyűzetekhez, egerekhez, távirányítókhoz és játékvezérlőkhöz. A remények szerint ez a szabvány a számítógépeken kívül a tévéknél, játékkonzoloknál, web tévéknél is el fog terjedni. Itt kétirányú 75 kb/s átvitel a követelmény, minimum 5 méter hatótávolsággal, amit egyszerre 8 különböző berendezés is használhat.

4.2 Bluetooth[11]

Viszonylag kevés olyan adatátviteli technológia létezik, melyről megálmodják, hogy egységesíti a piacot, majd azt valóban meg is teszi. Az Ericsson által 1994-ben megalkotott, az RS-232-es kommunikációs kábel leváltására létrehozott Bluetooth viszont pont ilyen. Manapság már szinte nincs olyan mobiltelefon, táblagép, Laptop és egyéb elektronikai mobil eszköz, amelyben ne lenne megtalálható a Bluetooth valamely változata. Ez a technológia ezekben az eszközökben már alapvető adatátvitelt tesz lehetővé, és többnyire már a 2.0 vagy a 2.1 es verziót használják.

4.2.1 A szabvány sikere

A Bluetooth sikere nem véletlen, több dolog szerencsés összejátszása kellett ahhoz, hogy eljusson oda, ahol most van. Bár alkotói munkája is mindenképp dicséretes, hiszen egy olcsón előállítható, meglehetősen alacsony fogyasztású kommunikációs csatornáról van szó, a siker nem feltétlenül ebben, hanem az autókban keresendő. Azért említem az autókat, mivel manapság már a legtöbb országban tiltják a mobiltelefon használatát vezetés közben, és így szükség volt olyan eszközökre, aminek a segítségével mégis tudunk beszélni útközben ismerőseinkkel, barátainkkal. Itt jönnek előtérbe a Bluetooth adatátvitelt használó headsetek, melyek a legpraktikusabb megoldást jelentik a problémára: jelentősen olcsóbbak az autókba beépíthető kihangosítóknál, használatuk pedig kényelmesebb, mint a készülékekhez kapott vezetékes headsetek használata.

4.2.2 Adatátvitel

A Bluetooth jelenleg legfeljebb 8 eszköz egyidejű kommunikációját teszi lehetővé úgynevezett *piconet* hálózatokban; ez a gyakorlatban annyit jelent, hogy a hárombites MAC címek használata mellett a 7 gép között van egy kiemelt (angolul *master*), mely bármikor bonthatja a kapcsolatot a többi géppel. Elméletben akár további 255 eszköz is lehet inaktív állapotban, melyeket a *master* bármikor aktívvá tehet. Piconet hálózatokat egyébként eredetileg az RN Nimbus számítógépeknél használtak. A Bluetooth jelenleg a 3.0-s verziónál jár, a mai mobiltelefonokban 1.2-es, 2.0/2.1-es és 3.0-s chipeket lehet találni, melyek 1, 3 és

[11] A rész elkészítéséhez Chris Hurley és tsi (szerk) - How to Cheat at Securing a Wireless Network, Syngress Publishing (2006) könyvet és http://mobilarena.hu/index.html weboldalt használtam.

24 Mbps-os elméleti maximális adatátviteli sebességet tesznek lehetővé. A Bluetooth hatótávolsága viszont nem a verziószámtól, hanem az osztálytól függ, az határozza meg ugyanis az eszközök teljesítményfelvételét; 3-as osztálynál 1, 2-esnél 10, 1-esnél pedig 100 méter a maximális hatótávolság, telefonokban a 2-est használják (maximum 2,5 mW felvétel). Mobiltelefonoknál a Bluetooth kompatibilitását elősegítendő az Open Mobile Terminal Platform (OMTP) nevű szervezett kiadott egy ajánlást, melyet a legtöbben mértékadónak ítélnek meg.

4.2.3 Headsetek használata

A Bluetooth headsetek-et két dologra tudjuk használni: telefonálásra és zenehallgatásra. Előbbinél bármilyen eszköz szóba jöhet, amiben van Bluetooth, egy headsetet gond nélkül csatlakoztathatunk notebookhoz, mobiltelefonhoz vagy GSM-modullal nem rendelkező PDA-hoz is, a lényeg, hogy az adott cucc ismerje a HFP-t (Hands-Free Profile). A zenehallgatáshoz viszont már szükséges az A2DP (Advanced Audio Distribution Profile) és az AVRCP (Audio/Video Remote Control Profile) profilok megléte is. Ezeket a legtöbb Bluetooth 2.0-s vagy 2.1-es készülék ismeri.

4.2.4 Multipoint

A Multipoint egy viszonylag friss fejlesztés a Bluetooth technológiában. Lényege, hogy segítségével egy headsetet egyszerre két eszközhöz (telefonhoz, számítógéphez) is hozzá tudjuk kapcsolni. Az ebből adódó előnyök egyértelműek: ha bejövő hívás jön, nem számít, hogy melyik hangforrásból érkezik, könnyedén fel tudjuk venni, nem kell állandóan cserélgetnünk a headsetet.

4.2.5 Bluetooth eszközök teljesítmény

A Bluetooth-os eszközök élettani hatása nem számottevő, ez azzal magyarázható, hogy ezeket az eszközöket eleve úgy tervezték, hogy alacsony legyen a teljesítményigényük, ugyanis ezek többségében hordozható eszközök elemeit illetve akkumulátorait használják. Ebből következően nem lehet nagy a teljesítményük sem. Sugárzási teljesítmény alapján három osztályba sorolták ezeket az eszközöket: 1-es osztály (100 mW), 2-es osztály (2,5 mW) és végül a 3-as osztály (1 mW). Ha ezeket a teljesítményeket összehasonlítjuk a GSM

telefonok által sugárzott teljesítménnyel, amely 900 MHz-en 2 W és 1800 MH-zen pedig 1 W, akkor láthatjuk, hogy még az 1800 MHz-en működő telefonok is jócskán meghaladják az egyes osztályok sugárzási teljesítményét.

4.2.6 A Bluetooth biztonsága

Minden Bluetooth eszköz négy alapvető tulajdonsággal rendelkezik, amelyek segítségével már a kapcsolódás kezdetekor biztonságra törekszik:

1. A Bluetooth eszköz címe, egy 48 bites cím, mely minden Bluetooth eszközben különböző.

2. A Saját azonosító kulcs, egy 128 bites sorozat, amit az azonosítási procedúrák során használ a készülék.

3. Saját kódoló kulcs, egy 8-128 bit hosszúságú kódolásra használt kulcs.

4. A készülék által generált véletlen szám, ami gyakran változik. A Bluetooth biztonság három szintre osztható:

- Nincs biztonsági intézkedés
- Szolgáltatások szintjén alkalmazott biztonsági intézkedések vannak
- Kapcsolat szintű biztonsági intézkedés van, amikor a biztonsági intézkedések már a kapcsolat létrehozatala előtt élnek.

Ezeken kívül persze előfordulhat, hogy az alkalmazások külön biztonsági intézkedéseket követelnek meg és alkalmaznak.

Bluetooth Kulcskezelése

A Bluetooth esetében több kulcstípust különböztethetünk meg. Egyrészt az összekötő kulcsokat (link keys), amik az alkalmazástól függően lehetnek kombinációs kulcsok, egység kulcsok, elsődleges kulcsok vagy inicializáló kulcsok. Másrészt pedig vannak a titkosító kulcsok (encrypting key). A biztonságos adatátvitelt az összekötő-kulcs biztosítja. Ez egy 128 bites kulcs, ami az authentikáció ideje alatt használatos, valamint részt vesz a titkosító kulcs létrehozásában is. A link key élettartama attól függ, hogy ideiglenes kulcsként lett-e létrehozva, amely az aktuális feladat elvégzése után megsemmisül, vagy többször felhasználható kulcsként lett definiálva, amit akkor kell használni, ha ugyanazt a feladatot többször is el kell végezni.

Titkosítás

A Bluetooth titkosító rendszere az átvitelre kerülő csomagok tartalmát titkosítja az E0 titkosító algoritmus segítségével, mely minden csomagot új folyamattal kódol.

A következő titkosítási módok fordulhatnak elő:

Ha egység kulcsot vagy kombinációs kulcsot használ, az adatátvitel nem lesz titkosítva, de ettől függetlenül a belső adatforgalom lehet titkosított.

Ha elsődleges kulcsot használ, három eset lehetséges:

- Egyáltalán nincs titkosítás;
- Az adatátvitel nem titkosított, de a belső adatforgalom az elsődleges kulccsal kódolt;
- Mindenféle adatforgalom titkosított az elsődleges kulccsal.

Titkosító kulcs: az éppen aktuális összekötő kulcs, egy 128 bites véletlen szám és az authentikációs folyamat során keletkező 96 bites szám részvételével és az E3 algoritmus segítségével jön létre, és automatikusan cserélődik, amikor a Link Manager aktiválja a titkosítást. Mivel a titkosító kulcsok mérete 8-128 bites intervallumban változik, szükségessé vált, hogy az eszközök közös megegyezéssel kiválasszák a kommunikációhoz használt kulcsot. A "tárgyalás" kezdetén a mester eszköz küld egy javaslatot a szolga eszközöknek, melyek ezt elfogadhatják, illetve javasolhatnak egy másikat. Ez addig folytatódik, míg valamelyik javaslat elfogadásra nem kerül. Legtöbbször a kisebb kapacitású eszközhöz igazodik a titkosító kulcs mérete, mivel ezek adatfeldolgozó képessége erősen behatárolt, így előfordulhat, hogy egy túl hosszú kulcsot nem tudnának lekezelni. A legtöbb alkalmazás megszab egy minimális kulcsméretet, melynek megléte nélkül nem használható. Ez kiszűri azon eszközöket, melyek nem képesek kellő biztonsággal kommunikálni, így is csökkentve a támadhatóság mértékét.

Authentikáció

Az Authentikáció gyakorlatilag az azonosítás. A Bluetooth eszközök az azonosítást kérdés-felelet formájában végzik el. A folyamat során használt protokoll szimmetrikus

kulcsokat használ, tehát a sikeres azonosítás azon múlik, hogy minden kommunikációban résztvevő eszköz ugyanazt a kulcsot tette-e publikussá a többi számára. Mintegy melléktermékként, az authentikáció során létrejön egy plusz számsor, amelyet a titkosítás folyamatában használ fel a Link Manager. A kapcsolódási kérelem megérkezése után először az azonosító fél küld egy véletlen számot a kérelmezőnek az azonosítás kezdetekor. Ezután mindkét eszköz alkalmazza a véletlen szám, az aktuális összekötő kulcs és a kérelmező eszközcímének hármasára az E1 függvényt, ami kiad egy értéket, az úgynevezett digitálisan aláírt választ (SRES). Ekkor a kérelmező elküldi a választ az azonosító félnek, aki megvizsgálja, hogy a megkapott SRES megegyezik-e az általa kiszámított értékkel. Ha igen, a kérelmező sikeresen azonosította magát. Amennyiben az azonosítás sikertelen volt, egy bizonyos időnek el kell telnie az új folyamat megkezdése előtt. Ez az idő minden egyes sikertelen kísérlet után megduplázódik, mígnem eléri a maximálisan megszabott várakozási időt. Legtöbbször a használt alkalmazás dönti el, hogy kinek kell azonosítania magát. Ez jelentheti a kérelmezőt, de előfordulhat, hogy a kiszolgálónak kell azonosítania magát. Ezeken az egyirányú azonosításokon kívül előfordulhat, hogy mindkét eszköztől megkövetelik az azonosítást.

Bluetooth biztonság lehetséges problémái

A Bluetooth titkosítási eljárásánál alkalmazott E0 bizonyos körülmények között egy bonyolult matematikai eljárással feltörhető, és ezzel lehetővé tesz egy "oszd meg és uralkodj" típusú támadást. Ez akkor lehetséges, ha a megadott kulcssorozat hosszabb, mint az E0-ban használt legrövidebb kulcssorozat tároló/feldolgozó regiszter (LFSR). Ez a támadási forma gyakorlatilag csak nagyon nehezen (vagy egyáltalán nem) kivitelezhető, mivel ehhez hozzá kellene férni a magas frekvencián (2.45 GHz) működő eszközben még magasabb frekvencián üzemelő kódgeneráló algoritmushoz, amikor az frissíti tartalmát. Ez az idő azonban olyan rövid, hogy szinte lehetetlen megszerezni. Csatlakozáskor minden résztvevő eszközbe külön-külön kell bevinni a PIN kódot. Ez egy nagyobb kiterjedésű ideiglenes hálózatban elég fárasztó lehet. Az inicializációs kulcs egy sebezhető pontja lehet a rendszernek, mivel az egyetlen titkos résztvevője a kulcs generálásának a PIN kód. Ha ez a PIN kód négyjegyű, egy bruteforce eljárással aránylag rövid idő alatt kikövetkeztethetjük a PIN kódot, és az E22 algoritmus ismeretében kiszámolhatjuk az inicializációs kulcsot. Ehhez még hozzájárul a humántényező is, miszerint a PIN kódok többsége a "0000" sorozat, illetve az illető születési

éve. Támadásra alkalmas hiányosság fedezhető fel az egység kulcs (unit key) kapcsán is. Tegyük fel, hogy A és B kommunikációjában A egység kulcsa az összekötő kulcs (link key). Most tegyük fel, hogy C is csatlakozik a kommunikációhoz és ő is A egység kulcsát használja összekötőként. Ekkor B, mivel már korábban összekötő kulcsként hozzáfért A egység kulcsához, egy hamis eszközcím megadásával kiszámíthatja a titkosító kulcsot és lehallgathatja az A és C közötti adatforgalmat (man-in-the-middle attack). A teljesen egyedi eszközcímek lehetőséget adnak az eszköztulajdonos szokásainak megfigyelésére és annak dokumentálására, ami sérti az illető személyiségi jogait. Az itt felsoroltakon kívül persze még akadhatnak hibák a rendszerben, mivel az átvitt adatok is rengeteg veszélynek lehetnek kitéve.

4.3 Near Field Communication (NFC)[12]

Az NFC technológia a Philips és Sony cégek együttműködéséből született 2002-ben. A fejlesztés során olyan megoldást kerestek mely könnyen használhatóvá és felhasználóbaráttá teszi a technológiát. Emellett fontosnak tartották egy globális méretű, érintés nélküli okoskártya olvasókészülék bázis kiépítését a vásárlói környezetben. Ennek következtében az új technológia kompatibilis a meglévő érintésnélküli okos kártyákkal. Az NFC technológiát előbb az ECMA, majd az ISO is elfogadta szabványnak. Az üzletági kísérletek 2004-ben indultak a Nokia, Motorola, Samsung és Siemens/BenQ cégek közreműködésével. 2004-ben megalakult az NFC Forumnak nevezett szövetség azon cégek társulásából, akik részt vesznek a technológia továbbfejlesztésében. Az alapítást a 2004-es CeBIT-en jelentette be a Sony, a Philips és a Nokia. A Forum immáron több mint 150 tagot számlál, melyek 4-féle kategóriába tartozhatnak: Szponzor, Vezető, Társ, Non-profit kategóriág vanak megkülönböztetve. A specifikáció részletei az ISO 18092-ben találhatók meg. A legfőbb tulajdonsága az NFC-nek az, hogy lehetővé tesz eszközök közötti vezeték nélküli kommunikációt 10 cm-en belül. Az NFC interfész különféle módokban működhet. A módokat a szerint lehet megkülönböztetni, hogy az eszköz generál-e rádiófrekvencia mezőt maga körül vagy az eszköz egy másik eszköz által létrehozott mezőt használ-e fel a kommunikációhoz. Az első esetben aktív eszköznek, a másik esetben pedig passzív eszköznek

[12]A leírás elkészítéséhez http://en.wikipedia.org/wiki/Near_field_communication és a http://mobilarena.hu/index.html weboldalt használtam

nevezzük a készüléket. A készülék lehet NFC tagkártyák, okos kártyák, címkék, és egyre több mai mobiltelefonba is kerül NFC. Az NFC mobiltelefonok mindkét módon működhetnek, köszönhetően a kártya-emuláció módnak. NFC egy a rádiófrekvenciás chipen alapuló vezeték nélküli, kis hatótávolságú kommunikációs technológia, mely 13,56 MHz-en működik. Működési távolság: körülbelül 10 cm, de ez erősen függ a megvalósítástól, a távolság az antenna átmérőjétől is függ. Adatátviteli sebesség 424 kbit/s, tervezett sebesség 1 Mbit/s. Kompatibilis a már közkedvelt érintésnélküli Mifare and FeliCa&trade okoskártya technológiákkal. A világon nagy mennyiségben fordul elő Mifare technológiára épülő eszköz infrastruktúra:

- 1,5 millió MIFARE olvasó terminál
- 250 millió MIFARE® kártya
- Az összes RFID standard tagkártya behatolását a piacra: 2006-ig a világon az egész érintés nélküli chip piac 87%-a az ISO 14443 szabványon alapult, 82%-át az A típusú kártyák, 5%-át a B típusú kártyák teszik ki. A maradék 13% megoszlása: 6% Sony FeliCa&trade, 7 % egyéb standardok.

Az ECMA340 szabvány leírás megfogalmazza az RF (Rádió Frekvenciás) interfész leírást, a kezdeti paramétereket, és a protokollt. Az NFC felhasználó oldali eszköz (mobiltelefon) két féle módon képes kártyaként működni:

- Nem biztonságos NFC: Mifare vagy FeliCa kártyát tud emulálni adott parancsok alapján, amit a vezérlő küld neki.
- Biztonságos NFC: a rádió frekvenciás eszköz tartalmaz SAM (Secure Access Module) chipet, ami egy speciális kártya emulációs szektort tartalmaz. Az ilyenfajta továbbfejlesztett eszköz képes felállítani egy biztonságos kommunikációs csatornát a már szabványosított titkosított rendszer alapján.

NFC számos területen megtalálható. elektronikus jegy, beléptetés, fizetés, érték-és csomagmegőrzés, Smart Poster. Ezeken a megoldásokon fellül rengetek mobiltelefon gyártó, azért is alkalmazza majd ezt a vezeték nélküli szabványt, mert ha beszerezzük otthonra az asztali számítógépünkhöz a megfelelő NFC-s eszközt, akkor egy kábel nélküli szinkronizációt is kapunk majd számítógépünk és mobiltelefonunk között.

4.4 GPRS, EDGE

4.4.1 GPRS (General Packet Radio Service)[13]

A GPRS (General Packet Radio Service) nagyjából az általános csomag alapú rádiós szolgáltatást jelent. A technológia 2001 óta érhető el, egy IP-alapú mobil átviteli eljárásról van szó, amely a GSM-szabványra épül. Az egyik első hazánkban is kapható GPRS-képes telefon az Ericsson R520M volt. A GPRS internetezésre azaz wap-ozásra szánták. Az elvi maximum sebessége 171,2 kbps, ezt azonban a gyakorlatban sosem lehet elérni, az elterjedt megoldásoknál a sávszélesség 30-70 kbps között mozog. A feltöltési ráta mindig alacsonyabb, mint a letöltési. A GPRS bevezetése komoly hálózatfejlesztési munkálatokat igényelt, lévén a szabvány magát a GSM-hálózatot használja, amit emiatt ki kellett bővíteni három új egységgel. Ezek az SGSN (Serving GPRS Support Node), amely a csomagkapcsolásért felel, GGSN (Gateway GPRS Support Node), amely egyrészt az SGSN-től kapott csomagokat alakítja át a megfelelő formátumúra, hogy a célhálózatok számára is értelmezhetőek legyenek, másrészt az ő feladata a bejövő csomagok címének átalakítása is. A harmadik kiegészítés a PCU (Packet Control Unit), amely a GPRS- és a hagyományos GSM-vonalak elkülönítéséért felelős. A GPRS-képes mobilkészülékeket két szempontból lehet osztályozni. Az egyik az úgynevezett *multislot*, ami azt adja meg, hogy a telefon maximálisan hány csatornát képes összekapcsolni, minél több van összekapcsolva annál gyorsabb sebességre képes. A legelterjedtebb a class 8, ahol 4 csatorna letöltésre 1 csatorna feltöltésre szolgál. A másik elterjedt a class 10, itt 4 csatorna letöltésre, 2 csatorna feltöltésre szolgál, de egy időben csak 5 csatorna üzemelhet. Léteznek 4+4 csatornás megoldások is, de ezekből is csak 5 darab csatorna használható egyszerre. Az osztályozásnál a második szempont a GPRS és a GSM együttes használatát vizsgálja, ebben három alkategóriát van. Az A csoportba tartoznak azok a mobil eszközök, amelyek képesek Dual Transfer módban működni, ami azt jelenti, hogy egyszerre képesek a GSM és a GPRS forgalomra. A B osztályba tartozó készülékek képesek mindkettőt használni, de az aktuálisan használaton kívüli felfüggesztett állapotba kerül. A C osztályba sorolt eszközök pedig egyszerre csak az egyik hálózatot képesek használni, tehát vagy a GPRS, vagy a GSM megy.

[13] Chris Hurley és tsi (szerk) - How to Cheat at Securing a Wireless Network, Syngress Publishing (2006)

4.4.2 EDGE (Enhanced Data Rates for GSM Evolution)[14]

A 2003 óta elérhető szabvány javított a modulációs eljáráson, a GPRS-hez képest háromszoros sebességre képes, igaz, emiatt sokkal rosszabb jel-zaj viszonnyal rendelkezik. A maximális sebesség függ a lefoglalt sávok (*slot*) számától, amely maximum 8 lehet ez egy fejlesztés a korábbi 5 csatornához képes, az elvi maximális sebesség 473 kbps nőt.

4.5 UMTS, HSPA, 4G

4.5.1 UMTS (Universal Mobile Telecomm[15]*unications System)*

Ahogy egyre jobban növekedett a sávszélességi igény, új szabványra volt szükség. Ezért kifejlesztették az UMTS-t, melyet 3G néven ismerünk. A rövidítés az egységes mobil telekommunikációs rendszert takarja. Ezzel a szabvánnyal egy egységes változatot akartak létrehozni, mert sajnos a GSM rendszerek sajnos komoly kompatibilitási gondokkal küszködtek, de ezt sajnos az UMTS-ben sem sikerült megoldani. Még további cél volt a hangminőség és az adatátviteli sebesség javítása. A sebességet sikerült a maximális 384 kbps-ra emelni. Fontos volt a kompatibilitás az előző generációval, valamint további új szolgáltatások bevezetése. Ilyen szolgáltatások például a csevegés, letöltések, videó telefonálás. Amikor elkezdték fejleszteni a hálózatokat akkor a régi tornyokat kikellett egészíteni az úgynevezett Node B csomóponttal, amely ugyanazt a szerepet látja el, mint GSM esetben a BTS (Base Transceiver Station), azaz ez kommunikál a környezetében lévő 3G-képes mobil eszközökkel. Mivel az UMTS 2100 MHz-es frekvencián üzemel, aminek kisebb a hatótávolsága, ezért szükség volt a tornyokat kiegészíteni. Ez a frekvencia okozza azt is, hogy a 3G jel nehezebben jut be beltéri területekre. A hálózatnak van még egy tulajdonsága, amit úgy hívnak egyszerűen, hogy "lélegzik". A bázisállomások ugyanis nagyszámú, egyidejűleg csatlakozó felhasználók esetén a toronyhoz közelebb eső igényeket szolgálják ki, azaz a lefedettség szélén próbálkozó ügyfelek ingadozó 3G jelerősséget

[14] A leírás készítéséhez Chris Hurley és tsi (szerk) - How to Cheat at Securing a Wireless Network, Syngress Publishing (2006) és a http://mobilarena.hu/index.html oldalt használtam.

[15] http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System

tapasztalhatnak. Az RNC (Radio Network Controller) vezérli az alá tartozó Node B-ket, az MGW (Media Gateway) pedig az adatátvitelért felel.

4.5.2 HSPA (High Speed Packet Access)[16]

A 3G utáni következő lépés a UMTS fejlesztése: HSPA, amit szokás 3,5G-nek is neveznek. Ez az elnevezés nagyából a magas sebességű csomagkapcsolti hozzáférést jelenti. Ez a szabvány két protokollt tartalmaz: az egyik a letöltési HSDPA, a másik pedig a feltöltési protokoll a HSUPA. A legkisebb letöltési sebesség eszköztől függően 1,8, 3,6, 7,2 vagy 14,4 Mbps is lehet; léteznek persze további fejlesztések, a cél a 42 Mbps (HSPA+) és a 84 Mbps (Release 9) körüli sebességek elérése. Feltöltésnél nyilván kisebbek a számok, de a UMTS Release 6-ban szereplő EUL (Enhanced Uplink) már 5,76 Mbps-ot is tud. Mindezt HSUPA néven lehet ismerni, a Release 9-es UMTS-nél egyébként 23 Mbps-ra fog gyorsulni a feltöltés.

4.5.3 4G

Az információtechnológia 4G-vel a negyedik generációs vezeték nélküli szolgáltatásokat jelöli. Ezt a rendszert, a szakértők szerint egy átfogó IP-infrastruktúra, nagy adatátviteli sebesség, nagy kapacitás és a nyílt internetes szabványok használata fogja jellemezni. A 4G-nél a mobil szélessávú rendszer továbbfejlesztett multimédiás szolgáltatásokkal bővül. Az IMT-Advanced, (4G Wireless and International Mobile Telecommunication) 4G technológia jelenleg a mobil távközlési rendszerek közül a legfejlettebb, amely fix környezetben 1 Gbps, mobilkörnyezetben pedig akár 100 Mbps adatátviteli sebességet is biztosíthat. Amit most a mobilszolgáltatók 4G néven bevezetnek, az valójában a 3,9G. Maguk a mobilszolgáltatók marketingesei találták ki azt, hogy adják ezt a nevet a hálózatnak. Az Egyesült Államokban, Németországban és Svédországban kiépülő LTE hálózat csupán néhány tíz megabites letöltési sebességet nyújt az ügyfeleknek. Egyelőre szó sincs száz és ezer megabitről.

[16] Chris Hurley és tsi (szerk) - How to Cheat at Securing a Wireless Network, Syngress Publishing (2006)

4.6 Home RF[17]

Az 1998-ban létrehozott Home RF technológiát a nevéhez híven, egy épület területén belüli rádiófrekvencián zajló kommunikációra, szélessávú otthoni vezeték nélküli Internet biztosítására optimalizálták, a maximális hatósugara 50 méter. Az átvitelre a 2.4 GHz-es ISM sávot használ, ebben az ipari- tudományos-orvosi célokra fenntartott frekvenciatartományban a sugárzáshoz nem kell engedély, a világ összes országában szabadon használható. Mivel ezt a frekvenciát sok egyéb eszköz is, mint például a mikrohullámú sütők, garázsajtó-nyitók is használják, nem kívánt interferenciák keletkeznek, ami elkerülése végett a Home RF FHSS-t alkalmaz 50-100 ugrás/másodperc ugrási sebességgel. A jó minőségű továbbított hangadat más frekvencián történő újraküldése, valamint az adatok 8 prioritási szinten való elhelyezésére adott lehetőség is. Az átviteli biztonságot 128 bites kódolási kulcs garantálja. Az első generációs készülékek párhuzamosan 4 aktív handset működését támogatták, a maximális átviteli sebesség 1.6 Mbit/másodperc volt. A 2001-es második generációs eszközök már 8 párhuzamos kapcsolatot képesek kezelni, az átviteli sebesség maximuma pedig 10 Mbit/másodpercre nőtt. Ennek 2002 második felére 20 Mbit/másodpercre növelése volt a cél. A méretben kicsi csak a Home RF technológiával elérhet Compact Flash Card a jelenleg elérhet legkisebb WLAN eszköz a világon, olcsó, energiatakarékos Home RF hálózati eszközökkel egyszerre használhatunk kliens/szerver és peer-peer, azaz a két felet egyenrangúan kezelő kapcsolatot is.

A technológia három típusú szolgáltatást támogat:

- 8 prioritási szintű kapcsolat orientált adatszolgáltatást
- aszinkron kapcsolat nélküli adatszolgáltatást
- szimmetrikus, full duplex DECT protokollnak megfelelő magas minőségű hangátvitelt

[17] A rész elkészítéséhez Wireless Security - The Newnes Know It All Series (2009), 172. old. és a Chris Hurley és tsi (szerk) - How to Cheat at Securing a Wireless Network, Syngress Publishing (2006) könyveket használtam.

4.7 HiperLAN2[18]

Manapság az Internet és különösképpen az intranetek elterjedésével egyre nagyobb az igény a szélessávú, nagysebességű vezeték nélküli adatátvitelre. A vezeték nélküli helyi számítógép hálózatok szinte mind az IEEE 802.11-es szabványon alapulnak. Mivel ezen eszközök egyre olcsóbbá válnak, egyre inkább a helyi számítógép hálózatok alternatíváját jelenthetik az Ethernet mellett. Azonban, hogy valódi alternatívát nyújtsanak ezek az eszközök, a nagyobb sávszélesség mellett szükség van QoS támogatásra, titkosításra, handoverre a helyi és cellás hálózatok között. A HiperLAN2 a vezeték nélküli helyi számítógép hálózatok egyik generációja. Az 5 GHz-es ISM sávban működik. HiperLAN2 nagysebességű adatátviteli sebességgel rendelkezik, tipikusan 6 Mbit/másodperc- 54 Mbit/másodpercig. Ez a technológia az ATM, IP és más szélessávú hálózatokhoz való vezeték nélküli hozzáférést biztosít. Alapvetően centralizált szervezésű, de fejlesztették az ad-hoc kiegészítést is mellé. Ekkor az MT-k közül választott úgynevezett Central Controler (CC) látja el az összehtwo9angolás feladatát. Mobilitást csak a lefedési területen belül támogat. HIPERACCESS kültéri, nagysebességű 25 Mbit/másodperc, fix rádió hozzáférést biztosít az előfizetői épületek között. Támogatja a multimédiás alkalmazásokat, más technológiák, pl. HiperLAN2 biztosíthatja az épületen belüli szétosztást. HIPERACCESS lehetővé teszi az üzemeltető számára nagy előfizetői területek gyors lefedését. Engedélyköteles vagy szabad sávban is működhet. Pl. az GHz-es sávot erősen támogatják. HIPERLINK igen nagysebsségű akár 155Mbit/másodperces adatátvitelt biztosít statikus rádió összeköttetésekkel és támogatja a multimédiás alkalmazásokat. Tipikus alkalmazása lehet a HIPERACCESS hálózatok és/vagy HIPERLAN AP-k összekötése egy teljes vezeték nélküli hálózatban. 17Ghz-en működik.

4.8 A 802.11

Az IEEE 802.11-ben fellelhető legtöbb fontosabb szabványára ki fogok térni, de az elején szeretnék egy kis rövid ismertetőt írni, hogy hogyan is fejlődött a 802.11. Az 1980-as években fejlesztették ki a vezeték nélküli LAN szabványt, és a három ISM rádiófrekvencián

[18] Elkészítéshez Wireless Security - The Newnes Know It All Series (2009), 172. old. könyvet és a http://ebookz.hu/ebook.php?azon=a04a10 linken elérhető jegyzetet használtam

lehetett használni engedély nélkül, 1985-ben már az FCC is használta. 1997 egy jelentős mérföldkő, mert ebben az évben tetszik közzé a 802.11 szabványt. Ez a szabvány, mely kezdetben csak szerény adatátviteli sebességgel bírt (1-2 Mbit/másodperc), az évek folyamán fejlődött. Megjelenik a 802.11a/b/g szabvány, 1999 júliusában kiterjesztették a 802.11a/b engedélyét, melyek sebessége akár 11 Mbit/másodperc (megabit: Mbit) lett és elkezdték forgalmazni az első ilyen szabványú termékeket. 2003 júniusában megjelenik a 802.11g szabvány, amely sebessége már elérte az 54 Mbit/másodperc sebességet és 2,4 GHz-es ISM sávon üzemelt.

4.8.1 A 802.11 MAC réteg[19]

A MAC (Media Access Control) réteg és a fizikai réteget a 802.11 protokollban vannak definiálva. A MAC alap funkciói közé a közeghozzáférés kezelése, titkosítás, és a szinkronizálás tartozik. A MAC rétegek által ellátott tipikus szabványos funkcionalitásokon túl a 802.11 MAC további funkciókat is ellát, melyeket tipikusan felsőbb rétegek szoktak például fragmentáció, csomag újraadás, nyugtázás. Az IEEE 802.11 szabvány egyetlen MAC-et definiál, ami 3 PHY (fizikai réteggel) tud együttműködni, amelyek 1 vagy 2 Mbit/másodperces átvitelt biztosítanak.

- Frekvenciaugratásos szórt spektrumú (Frequency Hopping Spread Spectrum,FHSS) a 2.4 GHz sávban
- Direkt szekvenciális szórt spektrumú (Direct Sequence Spread Spectrum, DSSS) a 2.4 GHz sávban és
- infravörös

Van az úgynevezett elosztott- DFC (Distributed Coordination Function): ahol a mobil terminálok ugyanazt az egyszerű szabályt alkalmazzák a rádiócsatorna megszerzésére, mindenféle központi „döntőbíró” nélkül, és az úgynevezett központosított- PCF (Point Coordination Function), ahol a terminálok kérései alapján az Access Point dönt a rádiócsatorna kiosztásáról, és a döntésének megfelelően adja meg a jogot az egyes mobil állomásoknak az adásra.

[19] Wireless Security - The Newnes Know It All Series (2009) 148-152. old.

MAC

Az alap közeg hozzáférési módszer a DFC alapvetően CarrierSense Multiple Access megoldásra épülő Collision Avoidance mechanizmussal kiegészítve (CSMA/CA). A CSMA protokollok jól ismertek az iparban, ilyen pl. az Ethernet, ami CSMA/CD módszer használ. Az adni kívánó állomás figyeli a közeget. Ha a közeg foglalt (másik állomás ad) akkor elhalasztja az adását egy későbbi időpontra. Ha a közeget szabadnak érzékelte, akkor megkezdheti. Akkor hatékony, ha a közeg nem túl terhelt, ilyenkor minimális késleltetéssel adhatnak, előfordulhat, hogy több állomás egyidejűleg szabadnak érzékeli a közeget és egyszerre kezd adni, ütközés keletkezik. Az ütközési helyzeteket fel kell tudni ismerni és így a MAC réteg újraadhatja a csomagot és nem a felsőbb rétegeknek kell ezzel foglakozni, ami jelentős késleltetést okozna. Ethernet esetén az ütközést az adó állomás ismeri fel és ezután egy úgynevezett újraadási fázisba megy át. A CD-t a WLAN-oknál nem célszerű alkalmazni. Collision Detection eljárás megvalósítása Full Duplex rádiós képességeket igényelnek, ami jelentősen növelné az árakat. Az ütközés érzékelése nehézkes, mert a saját jel elnyomja az esetleg távoli másik terminál kis teljesítményű jelét. A vezeték nélküli környezetben nem tételezhetjük fel, hogy minden állomás hallja a többit (ami a Collision Detection alapja), így a tény, hogy egy állomás szabadnak érzékelte a közeget, nem jelenti azt, hogy az a vevőnél csakugyan szabad is.

CSMA/CA

Az adni kívánó állomás érzékeli a közeget. Ha foglalt, akkor elhalasztja az adását. Ha szabad egy előre definiált ideig (Distributed Inter Frame Space, DIFS), akkor adhat. A vevő állomás ellenőrzi a vett csomag CRC-jét és nyugtát küld SIFS (Short Interframe Space) idő után (acknowledgment packet, ACK, MAC nyugta). A nyugta vétele jelzi az adónak, hogy nem történt ütközés. Ha az adó nem kapott nyugtát újra küldi a csomagot, amíg nyugtát nem kap vagy el nem dobja adott számú próbálkozás után. A SIFS azért kisebb, mint a DIFS, hogy a harmadik állomás ne kezdhessen el adni a nyugta elküldése előtt. Backoff-nak nevezik amikor minden állomás egy véletlen számot generál *n* és 0 között és a generált számnyi időrést (slot) vár mielőtt a közeghez fordulna. Egy állomás egy időrést választ, és ha az ütközik, akkor a véletlen szám generálás felső határát duplázza. Amikor az első átvitel előtt az állomás figyeli a közeget és azt foglaltnak találja, minden újraadás után vagy minden sikeres átvitel után.

Nem használandó ez az eljárás, ha az állomás adni kíván és előtte DIFS ideig szabadnak érzékelte a közeget. Késleltetési idő csökkentése akkor kezdődhet meg, ha a médium DIFS ideig szabad időrésenként eggyel csökkentik. Ez a folyamat egészen addig tart, míg a médiumon átvitelt nincs, ha van, a késleltetési idő csökkentése befejeződik a következő DIFS idejű üresnek érzékelésig. Egy terminál akkor adhat, ha a késleltetési ideje nullára csökken.

4.8.2 A PHY réteg[20]

Az 1997-ben engedélyezett 802.11 szabvány három alternatív PHY réteget támogat. Az egyik a frekvenciaugratás, a másik a közvetlen sorrendes szórt spektrumú rádiós összeköttetés és a harmadik az infravörös PHY. Az FHSS (Frequency Hopping Spread Spectrum, frekvenciaugratásos szórt spektrumú rádiós összeköttetés) esetén az adatátvitel frekvenciája folyamatosan pszeudovéletlen módon változik, amely szekvenciát mind az adó, mind a vevőállomás ismeri. Az eljárás biztonságosabbnak tekinthető, de megvalósítása bonyolultabb a DSSS-nél (Direct Sequence Spread Spectrum, közvetlen sorrendes szórt spektrumú rádiós összeköttetés). Beszélhetünk gyors FHSS-ről és lassúról. Az első esetben a bemenő adat „0” és „1” közötti váltása esetén is lehet frekvenciaváltás, a második esetben a váltás több nagyságrenddel lehet hosszabb időtartamú. A DSSS esetén az adatfolyam, egy nagyobb sebességű digitális kóddal szorozódik össze. Minden egyes adatbitet összeszorozódik az adó- és a kívánt vevőállomás által ismert sorozattal. Ezt az álvéletlen bitmintázatot chip kódnak nevezik. A kód magas és alacsony jelek álvéletlen sorozata. Dekódoláshoz az ismert álvéletlen kódsorozatot összeszorozva a kódolt jellel invertálva „0”-t kapunk, nem invertálva pedig az adatfolyam „1” értékét kapjuk.

[20] Wireless Security - The Newnes Know It All Series (2009) 153-158. old

4.8.3 Az IEEE 802.11 fejlődése[21]

IEEE 802.11a

Ez a szabvány a 802.11b–vel majdnem egyszerre jelent meg. Sok dologban eltér a ***B*** szabványtól. Legfontosabb, hogy 54 Mbit/másodperc (ez a gyakorlatban 21-22 Mbit) az elértő maximális sebessége, míg a ***B***-nek 11 Mbit/másodperc (ami a gyakorlatban 4,3 Mbit). Azért tudták elérni a nagyobb sebességet, mert 5GHz-es ISM sávban üzemel, tehát azok az egyszerű eszközök, amelyek rádiófrekvenciás hullámokat bocsátanak ki, nem zavarják az adatforgalmat. Hátránya azonban van a nagyobb frekvenciának, mégpedig könnyebben elakadnak a hullámok a különböző tárgyakban, falakon. Hatótávolsága ezért épületen belül 25 és 35 méter közé tehető. Ezt a távolságot talán ellensúlyozza az, hogy az 5 GHz-es tartományban több, egymást nem fedő csatornát vehetünk igénybe, akár egyszerre is. Ezzel a technikával növelhetjük sávszélességünket, hogy egyszerre több felhasználó nyugodtan internetezzen, másoljon hatalmas fájlokat, vagy akár nézzen filmeket (streaming), anélkül, hogy csökkenne a sebesség. Ezért az úgynevezett OFDM (Orthogonal Frequency Division Multiplexing, ortogonális frekvenciatartománybeli multiplexálás) moduláció felelős.
OFDM moduláció

IEEE 802.11b

A 802.11b szabvány sávszélességét tekintve 11 Mbit/másodper maximális adatátvitel sebességre képes, de az a gyakorlatban inkább 4 és 5 Mbit közé tehető. Ez a szabvány 2,4 GHz-es nyílt ISM sávon működik, mint például mikrohullámú sütőnk, vezeték nélküli telefonunk. Amiatt, hogy egy frekvencia sávon több eszközünk is üzemelhet, zavarhatják egymás rádióhullámait. Mivel kisebb frekvenciája, mint az ***A*** szabvány így épületen belül akár 38 méter, kint akár 140 méter is lehet. Található a szabványban DSSS (Direct Sequence Spread Spectrum). A DSSS kódolásnál minden átvinni kívánt bitet egy redundáns bitmintával helyettesítenek. Minél hosszabb ez a bitminta, annál nagyobb a valószínűsége, hogy az átviteli torzulások ellenére az eredeti jel helyreállítható. Illetéktelen megfigyelő számára a DSSS jel

[21] A fejezet elkészítéséhez a Wireless Security - The Newnes Know It All Series (2009) és a Chris Hurley és tsi (szerk) - How to Cheat at Securing a Wireless Network, Syngress Publishing (2006) könyveket használtam.

szélessávú kisenergiájú zaj. A legtöbb vezeték nélküli LAN eszközöket gyártó cég a DSSS eljárást választotta a kódoláshoz.

IEEE 802.11d

Ez a szabvány lehetővé teszi a MAC szintű konfigurációt, hogy be lehessen állítani a helyi előírásoknak megfelelő engedélyezett frekvenciát, teljesítmény szinteket, sávszélességet, ezáltal megkönnyítve a nemzetközi szabályokhoz való alkalmazkodást.

IEEE 802.11e

Ebben a szabványban megjelenik az úgynevezett QoS (Quality of Service, Szolgáltatás Minősége) eszköz. Ez a megoldás a hálózatok, hálózati eszközök és az erőforrások meghatározott rend szerinti felosztására, és garantált sávszélesség biztosítására van. A QoS-t támogató hálózatokon a magas prioritású üzenetek előnyben részesíthetők alacsonyabb besorolású társaikkal szemben, és konkurencia-helyzetben előbbiek továbbítása utóbbiak feltartóztatásával garantált sebességen biztosítható.

IEEE 802.11f

Ez a szabvány tartalmaz az IAPP-t (Inter-Access Point Protocol) mely a vezeték nélküli access pontok együttműködéséhez szükséges port. Engedélyezi az elérési pontok közötti cserét és támogatja az információ szétosztását a rendszerek között.

IEEE 802.11g

A 802.11g szabvány 2003-ban jelent meg, ugyan abban a tartományban üzemel mint a 802.11b, azonban megnövelt 54 Mbit/másodperces sebességgel rendelkezik, ami a gyakorlatban 19-20 Mbit/másodpercet sávszélességet jelent. tehát a 802.11a szabvánnyal azonos sebességű. A hatótávolsága a 2,4 GHz-es ISM frekvencia miatt beltérben körübellül 38 méter, kint 140 méter körül van. Még nagy előnye ennek a szabványnak, hogy visszafelé kompatibilis a 802.11b változattal, azaz ***G***-s eszköz képes kommunikálni ***B***-s Acces Point-tal, illetve ***B***-s eszköz ***G***-s Acces Point-tal. A továbbfejlesztett változatai: SuperG: 108Mbit/másodperc sebesség MIMO (multiple in, multiple out), több antennával a rádióhullámok visszaverődését is képes értelmezni, ezért nagyobb lefedettséget biztosít.

IEEE 802.11h

Spektrumgazdálkodás az 5GHz-es ISM sávban, található benne egy eszköz, ami a dinamikus frekvencia kiválasztásért felelős ez a DFS (Distributed File System) és megtalálható benne az átviteli teljesítményt szabályzó TPC is. Ezek arra jók, hogy megfeleljenek az európai követelményeknek, és legkevésbé akadályozzák a katonai radarokat, és a műholdas kommunikációt.

IEEE 802.11i

Megjelöli a biztonsági hiányosságokat, amelyek felmerülnek a felhasználói hitelesítési és titkosítási folyamatok során. Ez a változat tartalmaz egy magasabb szintű titkosítási formát - ez az AES (Advanced Encryption Standard) - a 802.1x hitelesítési forma mellett. Az AES egy 256 bites block-cipher kódolási eljárás. Átveszi a 40- és 128 bites stream-cipher RC4 eljárás helyét, amiket az elődök - Wired Equivalent Privacy (WEP) és WiFi Protected Access (WPA) - használtak.. Az RC4 egy stream-cipher mechanizmus, ami annyit jelent, hogy generál kulcs-streamet, ami ugyanakkora, mint az adat-stream. Egy 200 byteos adathoz egy 200 byteos kulcs párosul. Nagyon nehézzé válik a biztonságossá tétele brute-force típusú támadásokkal szemben. A másik oldalon a block-cipher az adatokat és kulcsokat blokkokra szedi szét. Mindegyik blokkot fel kell törni, külön-külön. Így sokkal több támadást kell intézni a hálózat ellen. A számítások szerint 100 év lenne feltörni az AES-t. A kódolás erősségével párhuzamosan a 802.11i-nek van beépített MAC fejléc védelme (ami az RC4-ben nincs). A 802.11 Message Integrity Check (MIC) protokol összehasonlítja a MAC fejléceket küldéskor, illetve vételkor, amennyiben különbözik a kettő, a csomagot eldobja, ezáltal megakadályozza a man-in-the-middle típusú támadásokat. A meet-in-the-middle (középen találkozás) egy kriptográfiai támadás, amelynek során egy két függvény kompozíciójából álló titkosítást ismert nyílt és kódolt szöveg birtokában úgy támadnak, hogy eltárolják a nyílt szöveg első függvény szerinti titkosításával, és a kódolt szöveg második függvény szerinti visszafejtésével kapott szövegeket. Egyezés esetén sikerült feltörni a titkosítást.

IEEE 802.11j

Japán szabályozás a 802.11a kiterjesztése hozzáadva a 4.9 és 5 GHz-es rádió frekvencia közé.

IEEE 802.11k

A 802.11k jelű szabvány nem – a ***A,B,G*** szabványokhoz hasonló jellegű – sebesség illetve egyéb átviteli jellemzők újabb lefektetése, hanem a jelenlegiek szerint működő eszközök lehetőségeit bővíti ki. Ebből következik az, hogy a megoldás szoftveres alapú, így a legtöbb ***A,B,G-es*** eszközt el lehet látni a szabvány által szabályozott képességgel. Amennyiben a szolgáltató eszközök (elsősorban Access Point) és a kliens eszközök is ismerik a szabványt, úgy képesek egymással a fizikai helyzetre és az aktuális hálózati leterheltségre vonatkozó információkat kicserélni, illetve kapcsolat megszakítás nélkül lehetőség nyílik az úgynevezett roamingra, azaz a kliens minden további nélkül válthat hozzáférési pontot. Ezen információk birtokában a kliens eszköz képes eldönteni, hogy ha több hozzáférési pontra képes csatlakozni, akkor számára előnyösebb, ha gyengébb jelerősséggel csatlakozik egy kevésbé leterhelt ponthoz, vagy egy nagyon leterheltre, aminek jó a jelerőssége, és lehetőség szerint mindig az optimális megoldást választja. Mobil felhasználás esetén pedig optimális időpontban vált a kapcsolat megszakítása nélkül hozzáférési pontot. Az információgyűjtés, és csere az OSI modell szerinti 1-es és 2-es szinten történik. Az információ tartalmazza az aktuális hozzáférési pontra vonatkozó kliensek számát, az általuk lefoglalt erőforrásokat, esetleges további pontokra, illetve az RF csatornákra vonatkozó adatokat Tartalmazza a hálózatok teljesítmény optimalizálását és a csatornaválasztást. A teljes hálózati teljesítmény is maximálva van, hogy a leghatékonyabban kielégítsen minden hozzáférési pontot a hálózatban.

IEEE 802.11n

Manapság ez a szabvány már minden frissen piacra került eszközben szinte biztos, hogy benne van. 2009 októberében jelent meg ez a változat 2,4 és 5 GHz-es ISM sávon is működik maximális sebessége 600 Mbit/másodperc melyet a MIMO-nak (Multiple Input, Multiple Output) köszönhet. Egyetlen jel duplázása vagy erősítése helyett több, különálló jelet alkalmaznak, azaz egyszerre több hálózati kapcsolat épül ki az adó és a vevő között. Mivel teljesen elkülönülő jelekről van szó, kevésbé zavarják egymást, és jelentősen megnövekszik a hasznos sávszélesség. Az N szabványt alkalmazó WiFi-s routereknek általában kettő antennájuk, de sok esetben akár három antennájuk is van. Épületen belül közel 70 méter, épületen kívül akár 250 méter is lehet a hatótávolsága. A másik fonto változtatás a 40 MHz-es csatorna implementálása. Az eredeti terveket módosítva az új verzió képes a

korábbi 2,4 GHz-es sávot használó eszközöket kezelni úgy, hogy két 20 MHz-es frekvenciát használ egymás mellett. Az új szabvány szerint a rendszer folyamatosan figyeli, vannak-e a környezetében olyan régebbi eszközök, melyek nem képesek kezelni a szélesebb sávszélességet. Ha talál ilyet, a 802.11n eszköz leszabályozza önmagát, és csak az egyik 20 MHz-es sávon küldi az adatokat.

IEEE 802.11p

A vezeték nélküli hozzáférés a közlekedési környezetben, vagyis ez a szabvány az úgynevezett WAVE (Wireless Access for the Vehicular Environment, vezeték nélküli elérés járművek számára). Kifejezetten mozgó járművekben történő felhasználásra terveztek.

IEEE 802.11r

A 802.11 vezeték nélküli szabványok infrastrukturális hátterét eredetileg azzal az elgondolással alkották meg, hogy a hálózati hozzáférést szolgáltató központi egységhez egyszerre több kliens csatlakozhasson -- az eszközök viszont nem kommunikálhatnak egyszerre több bázissal. A hozzáférési pontok közti zökkenőmentes váltás ugyanakkor elvileg biztosított, bizonyos alkalmazási területeknél azonban túl hosszúnak bizonyult az eddigi szabványokban meghatározott, 100 milliszekundumos újraszinkronizálási idő, ráadásul a kapcsolat teljes felépüléséig gyakran hosszú másodperceket kellet várni, különösen, ha titkosított a kommunikációs csatorna. A 802.11r WiFi szabvány, lehetővé teszi a vezeték nélküli bázisok közti "roamingot". A szabvány tartalmazza a Fast Basic Service Set Transition (gyors alapszolgáltatás beállítási váltás) technológiát, amely képes egy meglévő biztonságos kapcsolat aktívan tartására. Ezt úgy teszi, hogy előre meghatározza a következő bázisra csatlakozáshoz szükséges biztonsági paramétereket még a csatlakozás előtt. Ezzel lecsökkenti az átcsatlakozásra szükséges időt és képes megtartani a meglévő, időre érzékeny biztonságos kapcsolatot. A megoldás hasznos lehet privát hálózatokon, de igazán előnyös inkább a VoIP alkalmazások terén, ahol nagyon fontos a kapcsolat stabilitása vezeték nélküli bázisok közti váltáskor.

IEEE 80211.s

A vezeték nélküli IEEE 802.11 szabvány egy Mesh szerkezettel lett kiegészítve. A 802.11s szabvány célja egy olyan protokoll létrehozása, mely önállóan tudja konfigurálni az

útvonalakat az elérési pontok között egy "mindenki mindenkivel" felépítésben. Az ilyen hálózat alapelve az elérési pontok olyan széthelyezése és egy hálózattá kapcsolása, hogy mindegyik csomópontja kapcsolatot tudjon létesíteni a szomszédos pontokkal. Csak a végső kapcsolóelemet kell egy állandó hálózatra, pl. az Internetre kötni. A Mesh hálózat felépítése egy decentralizált hálózaton alapul, relatíve olcsó és a legfontosabb előnye a megbízhatóság. A hálózat mindegyik csomópontja több szomszédos pontból és pontba vehet, illetve küldhet át üzeneteket. Ezért, ha az egyik csomópont kapcsolása megszűnik, a hálózat automatikusan újabb utat keres az adatok továbbítása számára. A standard WDS módtól eltérően a Mesh routerek automatikusan azonosítják szomszédjaikat és tanulják ki a legegyszerűbb elérhetési útvonalakat. Nem kell ezért manuálisan konfigurálni az elérési pontokat. A rendszer e bizonyos fokú "önirányítása" csökkenti a rendszerbővítési költségeket. A Mesh hálózat felépítését rugalmasság, biztonság és integritás jellemzi. Azonban a megfelelő hivatalos szabvány hiányában a különböző gyártók elérési pontjai nem biztos, hogy kompatibilisek lennének egymással. Az IEEE 802.11s szabvány megteremtése ezt a helyzetet hivatott elkerülni.

IEEE 80211.T

Ajánlott gyakorlatokat, mérési módszereket, teljesítménymutatókat és vizsgálati eljárásokat tartalmaz ez a szabvány. Ezekkel mérik fel a 802.11 berendezéseket és hálózatokat. Ez a változat tartalmazza a WPP-t (Wireless Performance Prediction, vezeték nélküli teljesítményjóslást.

IEEE 802.11u

Módosítja a fizikai és a MAC réteget. Ez a szabvány előírás követelményeket tartalmaz a következőkben, hálózat kiválasztása, segélyhívás támogatása, sürgősségi riasztási és a felhasználói forgalom szegmentáció. Az IEEE 802.11 szabvány azt feltételezi, hogy a felhasználó készüléke engedélyezett a vezeték nélküli hálózat használatára. A 802.11u szabvány kiterjed azokra az esetekre, amikor a készülék nem előre engedélyezett egy adott hálózaton. A hálózat képes lesz arra, hogy hozzáférhetővé tegye a felhasználó számára a külső hálózatot, vagy jelzi, hogy online belépés lehetséges, vagy a hozzáférést szigorúan korlátozza, és így csak például segélyhívás lesz csak elérhető.

IEEE 802.11v

Az IEEE 802.11 szabványoknál nem figyeltek oda az energiatakarékoskodásra, ez a változat tartalmaz energiatakarékossági funkciót. Az egyik funkció közé tartozik a vezeték nélküli hálózatok alvó üzemmódja. Ez aszt teszi lehetővé, hogy hibernálva legyen a vezeték nélküli készülékünk, amivel energiát takarít meg, mint a hagyományos router-ek. A 802.11v változat képes arra, hogy felhasználói beavatkozás nélkül a készenléti állapotból felébredjen. E mellet a energia takarékossági funkció mellett rendelkezik olyan funkcióval, ami erősíti a hálózati teljesítményt, és a biztonságot.

IEEE 802.11w

Ezzel a szabvány azokat a biztonsági réseket akarják javítani, amik felmerültek az előző 802.11i változatnál és ezzel jelentősen megnőne a vezeték nélküli hálózatok biztonsága. A MAC (media access control) rétegen elvégzett módosításokkal, titkosítással a jelenlegi 802.11, köztük a 802.11i szabványnál is erőteljesebb védelmet biztosít. A rendszerek azért támadhatóak, mert a menedzseléshez szükséges adatkeretek még mindig védelem nélküliek.

IEEE 802.11y

Ez a szabvány 2008 szeptemberében jelent meg, fő különlegessége a hatalmas hatótávolsága, amit kinti környezetben lehet igazán kihasználni, akár 5000 méteres hatótávolságot is el lehet érni ezzel a 802.11 változattal. Épületen belüli hatótávolsága 50 méter körüli. Ez a szabvány a többitől eltérően nem 2,4 GHz-es vagy 5 GHz-es frekvencián működik, hanem 3,65-3,7GHz ISM sávon működik. A hatalmas hatótávolság ellenére is 54 Mbit/másodperces a maximálisan elérhető sebesség, ami a gyakorlatban 23 Mbit/másodperc.

5 Biztonság: Támadások és kockázatok

Amikor már van egy kiépített vezeték nélküli hálózatunk otthonunkban, sokkal kényelmesebb használni az eszközöket, melyekkel nem vagyunk adott helyhez kényszerítve, kényelmesen áthelyezhetjük vezeték nélküli eszközinket máshová, és folytathatjuk onnan munkánkat, internetezésünket, szórakozásunkat. Felmerül a hordozhatóságnak egy hatalmas előnye, de a másik oldalról sem árt belegondolni, hogy védenünk kell a hálózatunkat. A vezetékes otthoni hálózatoknál az eszközök kábelek között kommunikálnak, ezekre egy nem engedélyezett felhasználó nem tud rácsatlakozni, mert ahhoz neki is vagy rá kéne csatlakozni a hálózati elosztónkra, vagy olyan közel kéne férni a kábelekhez, hogy lehallgathassa azt egy eszközzel. A WiFi-s eszközök megjelenésével, ez a probléma azonban igenis megjelenik, mert az eszközök között nem kábelek szolgáltatják a csatornát, hanem a levegő, és a két eszköz között így szabad a csatorna, és távolabbról, akár 50-100 méterről is lehallgatható lesz a hálózatunk. Ehhez a csatornához az arra nem jogosult felhasználók sokkal hamarabb és kényelmesebben, akár a szomszédból, vagy utcáról is hozzáférhetnek. Tehát ha nincs megfelelően védve vezeték nélküli hálózatunk, igen hamar mások kezébe kerülhetnek bizalmas adataink, eszközeinkről állományaink. Egy vezeték nélküli hálózathoz nem kell közel elhelyezni semmilyen eszközt, amivel a lehallgatást végeznénk elég, ha a hálózat hatókörzetében tartózkodunk, és egy hálózati kártyával, amely alkalmas WiFi-s jelek vételére, lehallgatjuk a csatornát. Igazából a hálózatok lehallgatása és a hálózathoz illetéktelenek csatlakozása minden hálózat típusnál fenn áll, de a vezeték nélküli hálózatoknál ezek sokkal gyakoribbak. Természetesen mindkét hálózat esetén lehetőség van ezen problémák kiküszöbölésére vagy a kockázatoknak megfelelő mértékű enyhítésére, adminisztratív és műszaki eljárásokkal, intézkedésekkel.

5.1 Támadási módok

5.1.1 Sniffer - Csomagok lopása[22]

A sniffer egy olyan szoftver, amely képes elkapni a hálózatra kapcsolódó számítógépeken folyó adatforgalmat. Többféle platformon is futtatható. Az egyszerűbb változatai a szoftvernek parancssorból kezelhetőek, és a képernyőre kiírják az elkapott adatokat. Az összetettebb verziók már grafikusak forgalmi statisztikákat jelenítenek meg, és különböző beállítási lehetőségeket nyújtanak. A snifferek más programok számára motorként is szolgálnak, az IDS (Intrusion Detection System, behatolás figyelő rendszerek) is ezeket használják, hogy egyeztessék a hálózati csomagokat az eltárolt szabályrendszerrel. Ezek a rendszerek különös vagy veszélyes csomagok után kutatnak. A hálózatfigyelő szoftverek gyakran épülnek a snifferekre, hogy megszerezzék az analízishez szükséges adatokat. Tudva azt, hogy a snifferek egyszerűen elkapják a hálózati adatforgalmat. A snifferek működését az teszi lehetővé, hogy például internetes böngészés közben a számítógépek állandóan kommunikálnak egymással. A felhasználók képesek figyelemmel követni a számítógépek be illetve kimeneti adatforgalmát. Emellett a legtöbb számítógép helyi hálózatba van kötve, azaz több számítógépes eszközzel osztják meg a kapcsolatot. Az ilyen hálózat, ha nem kapcsolt (azaz nem switchekre, hubokra kapcsolódnak a gépek), egy csomag, melyet egy szegmens adott gépének címeznek, a szegmens összes gépén keresztülmegy. Ez azt jelenti, hogy egy számítógép tulajdonképpen az egész hálózat adatforgalmát látja, de semmibe veszi, hacsak más utasítást nem kap. Most már láthatjuk, hogyan is működik egy sniffer, megmondja a hálózati kártyának, hogy ne vegye semmibe a többi számítógépnek címzett forgalmat, hanem figyeljen rá. Ez úgy érhető el, hogy a hálózati kártyát úgynevezett válogatás nélküli módba kapcsolja, ez root, vagy adminisztratív jogot igényel. Amint a hálózati kártya ilyen állapotba kerül, a számítógép látja az egész szegmens adatforgalmát. A program ezután elkezdi olvasni a beérkező információkat. Az adatok különféle formában mennek a hálózaton, például csomagokban, frame-ekben, vagy más specifikált formátumban. Mivel ezek a szabályok szigorúan kötöttek, a sniffer szét tudja válogatni, és utána dekódolni a lényeges információkat. Mivel egy hálózatnál csomagok ezrei cserélődnek, a különböző eszközök között, ez bőséges adatot jelent egy illetéktelen támadó számára. Majdnem minden adat sebezhető, amit a

[22] Chris Hurley és tsi (szerk) - How to Cheat at Securing a Wireless Network, Syngress Publishing (2006)

hálózaton két eszköz átküld, jelszavak, web csomagok, adatbázis-lekérdezések. Egy sniffert könnyedén be lehet arra állítani, hogy egy forgalmat figyeljen, például emaileket. Miután a forgalmat lehallgatta, a hacker gyorsan hozzájuthat a számára szükséges információkhoz például jelszavakhoz és felhasználó nevekhez. Ezt a felhasználók többnyire sohasem tudják meg, hogy mi is történt, hiszen a snifferek nem okoznak károkat vagy zavart a hálózat működésében.

5.1.2 Access Point lemásolás

A vezeték nélküli hálózatok támadásának egy másik típusa az úgynevezett Access Point klónozás. A támadás annyiból áll, hogy egy kiválasztott Access Point-ot kell lemásolni. A MAC címét lemásoljuk az Access Point-nak és az SSID azonosítóját, majd mintha a klónozott AP lenne az eredeti, elkezdünk vele sugározni és a későbbiekben a kliens erre az AP- ra próbál majd fellépni. A kapcsolódás során minden, olyan információt megkaphatunk, ami az eredeti AP-hoz való hozzáféréshez szükséges. EZ a módszer akkor nem működik, ha vállalati autentikációt (RADIUS szerver) használ az eredeti Access Point. A RADIUS szerver (Remote Authentication Dial In User Service) egy a pre-paid rendszerbe integrált UDP kommunikációra épülő radius protokollt megvalósító komponens. A standard radius protokoll által definiált, AAA (authentication, hitelesítési; authorization, engedélyezési; accounting, elszámolási) típusú üzenetek fogadására és küldésére képes, és az AAA feladatokat látja el a PP szerverrel közösen. A hagyományos kliens szerver architektúrára épülő radius kliensek (Network Access Server-ek) minden egyes kérését önálló session-ként kezelő modellre épül. Csak a konfigurációs file-ban előre bejegyzett Network Access Server-ektől fogad el üzeneteket. Lehetőséget ad az üzenetek titkosítására szolgáló shared secret-ek megadására is.

5.1.3 Brute Force támadás[23]

A Brute Force támadás a teljes kipróbálás módszerét is jelenti, egy a titkosított rendszerek feltörésére alkalmazott módszer, mely többnyire sikeres. A rejtjelező rendszer ismeretében az összes lehetséges kulcsot kipróbálva keresi meg a megfelelő kulcsot. Eredményességét csak a számítógépes eszközök gyorsasága, teljesítménye határozza meg. A feltörési idő függ a lehetséges kulcsok számától, azaz a kulcs hosszától, és a választható

[23] http://en.wikipedia.org/wiki/Brute-force_attack

karakterek típusától. Legfőbb nehézséget az okoz, hogy a kipróbált kulcsról eldöntsük, hogy jó-e vagy rossz. A kulcsok száma = (karakterek száma) $^{\text{kulcs hossza}}$

Megfelelően úgy tudunk a Brute Force támadások ellen védekezni, ha a hozzáférési pontok jelszavát folyamatosan cseréljük.

5.1.4 Man-in-the-middle attack[24]

Man-in-the-middle attack, magyarul középre állásos támadásnak hívjuk. A középre állásos támadás során a két fél közötti kommunikációt zavarja egy támadó, úgy hogy a csatornát eltérítve mindkét fél számára a másik félnek adja ki magát. Így a korábban beszélgető két fél, innentől kezdve azt hiszik, hogy továbbra is egymással beszélgetnek, miközben mindketten a támadó vannak csak kapcsolatban. A támadó így kijátszhatja az ilyen támadásokra fel nem készített protokollokat. Ahhoz, hogy egy Man-in-the middle attack sikeres legyen, a támadáshoz a támadónak hozzá kell férnie a csatornához, amelyen a kommunikációt folytatják, és képesnek kell lennie lehallgatni az azon küldött üzeneteket és megakadályozni, hogy eljussanak a valódi címzettnek. A támadó ezt telepített WiFi bázisállomás segítségével teheti meg. Kivédésre rendszerint valamilyen nyilvános kulcsú titkosításon alapuló azonosítási rendszert használnak.

5.1.5 Wardriving[25]

A wardrivign egy olyan folyamat, amelynek keretében olyan vezeték nélküli hálózatok után kutatnak az hackerek, amelyek nincsenek levédve, vagy kis kódolással rendelkeznek, ezért oda be tudnak lépni. Sajnos ez a tevékenység manapság kezd egyre népszerűbbé válni az emberek körében, ezért fontos, hogy otthoni hálózatainkat próbájuk minél biztonságosabbá tenni. A wardriving kezdetben nem arra szolgált, hogy mások vezeték nélküli hálózatára felcsatlakozzanak a jogosulatlan felhasználók és használják a hálózat internet elérését, vagy más személyes adataihoz hozzájussanak, ez eleinte a hálózatok nevének és helyzetének felderítésének örömére szolgált. Az ilyen hálózatokba való belépés nem minden esetben törvénytelen, de ha tudjuk bizonyítani, akkor sok esetben fordulhatunk bírósághoz, hogy illetéktelenek törtek be privát hálózatunkba. A másik oldalról nézve lehet, hogy nem

[24] http://en.wikipedia.org/wiki/Man-in-the-middle_attack

[25] Chris Hurley és tsi (szerk) Wardriving and Wireless Penetration Testing Syngress Publishing (2006)

törvénytelen, de etikátlan, mert mások informatikai eszközeit, és a mások által fizetett sávszélességet használják, és személyiségi jogi kérdéseket is felvet, hiszen ez által a wardriver mások személyes adataihoz fér hozzá. A folyamat közben általában mozgásban vannak a hackerek, ha gyalog mennek, warwalkingnak, ha biciklivel, akkor warbikingnak nevezik ezt a tevékenységet. Aki a wardriving folyamatot végzi az a wardriver. Amikor nyitva hagyott hálózaton internetezik valaki, azt piggybackingnak nevezik. Nagyon sok esetben maguk az tulajdonosok sem figyelnek eléggé, hogy megfelelően titkosítsák a hálózatukat, egy 2005.09.11-én, Budapesten készített statisztika alapján 896 hálózatból 176 WPA2 titkosítású, 222 WEP titkosítású, és 498 tehát több mint a fele nyitott hálózat volt. Természetesen most már ezek az arányok javultak, és átfordult az arány, hogy több titkosított hálózat van, mint nyitott, melyre könnyedén fel lehet csatlakoznia bárkinek, de ezek a hálózatokon még mindig nem a legmegfelelőbb védelem van. Magyarországon nem rosszabb a helyzet, mint külföldön, sok a titkosított hálózat (többnyire WEP és WPA2), MAC filterezés és SSID broadcast tiltás jellemző, a rendes autentikációs megoldás nagyon ritka.

5.1.6 MAC lopás

Vannak az úgynevezett hozzáférési listák, amelyek routerekben illetve switchekben használható az interfészek közötti forgalom korlátozása céljából. A cél lehet forgalmi terhelés csökkentő, illetve biztonságot fokozó. Az ACL-ek (Access Control List) utasításlisták, melyeket egy forgalomirányító-interfészre alkalmazunk. Ezek a listák megadják a forgalomirányítónak, hogy milyen csomagokat fogadjon el és milyeneket utasítson vissza. Az elfogadás és a visszautasítás alapja lehet például a forráscím, a célcím vagy a port szám. A hozzáférési listák a forgalomirányító-interfészekre történő alkalmazásukkal lehetővé teszik a forgalom felügyeletét és meghatározott csomagok ellenőrzését. Minden forgalmat, amely áthalad egy interfészen, ellenőriznek a hozzáférési listában megadott feltételek alapján. A MAC magyarul egyedi hálózati azonosítók (Media Access Control Address esetében sajnos más a helyzet, mint a hozzáférési pontoknál. A MAC címek egyszerűen ellophatóak, akkor is ha WEP titkosítást használunk vezeték nélküli hálózatunkon. Egy másik hatalmas probléma, hogy a MAC címeket nagyon egyszerűen lehet megváltoztatni szoftveres úton. A támadók többnyire ezeket az a hibákat használják ki, és előnyükre fordítják, amikor feltörnek egy hálózatot. Ekkor egy valódi MAC címet szimulálnak a vezeték nélküli kártya programozásával, hogy bejussanak a támadók. A MAC címek hamisítása nagyon egyszerű,

egy speciális csomaglopó programot ráállítanak a hálózatra, és figyelik a csomagokat, és a támadó találhat egy működő MAC címet, és a vezeték nélküli eszköz MAC címét át is állíthatják a csomagokból kiszűrt címre.

5.1.7 Access Point spoofolás[26]

Az Access Pointokat lehet spoofolni, ami annyit jelent, hogy ha a vezeték nélküli hálózatunkhoz közel van egy hacker vezeték nélküli eszköze, akkor megvalósítható ez a folyamat. A hozzáférési pontot be kell állítania a támadónak, hogy jelet sugározzon a közelben lévő eredeti vezeték nélküli hálózathoz, és a lényege az, hogy a támadó jele erősebb legyen, az eredeti vezeték nélküli hálózat hozzáférési pontjánál, hogy a hálózat felhasználó eszköze a támadó jelet nézze eredetinek. A támadó jelet, ha eredetinek nézi a felhasználó vezeték nélküli eszköze, akkor ahhoz próbál majd csatlakozni, miközben a felhasználó létrehozza a kapcsolatot, a támadó hacker ellophatja a jelszavát, a hálózati hozzáférést. Ezt a támadási típust többnyire jelszószerzésre alkalmazzák a támadók.

5.2 Biztonságot növelő eszközök

5.2.1 WEP[27]

A Wired Equivalent Privacy elnevezés magyarul vezetékessel egyenértékű biztonságú hálózatot jelent, mára már egy igen elavult algoritmus, a 802.11-ben megfogalmazott vezeték nélküli hálózatok titkosítására szolgál. Fontos, hogy a vezeték nélküli hálózatok megfelelő védelmi mechanizmusokkal legyenek ellátva, melyek minden körülmények között, vagyis rosszindulatú támadások esetén is biztosítják a biztonságos működést. A WEP célja az, hogy a vezeték nélküli hálózatok legalább olyan biztonságosakká váljanak, mint egy biztonsági kiegészítésekkel nem rendelkező vezetékes hálózat. Ha egy támadó egy vezetékes Ethernet hálózathoz szeretne csatlakozni, akkor közvetlenül a hálózat közelében kell lennie, és kábellel hozzá kell, hogy férjen a vezetékes eszközhöz. A vezetékes hálózatokat a támadó szemszögéből nehezebb elérni. Ezzel szemben egy védelmi mechanizmusokat nélkülöző

[26] Wireless Security - The Newnes Know It All Series (2009)

[27] Chris Hurley és tsi (szerk) - How to Cheat at Securing a Wireless Network, Syngress Publishing (2006)

vezeték nélküli LAN-hoz való hozzáférés a rádiós csatorna nyitottsága miatt triviális feladat a támadó számára. A WEP ezt a feladatot hivatott megnehezíteni. Fontos megjegyezni, hogy a WEP tervezői nem törekedtek „tökéletes” biztonságra. Amikor már eredetileg tervezték a WEP-et, nem figyeltek igazán oda arra, hogy a biztonságot tényleg magas szintre emeljék. Ezért, ahogy a WEP megjelent, pár éven belül súlyos biztonsági hibákat találtak és nyilvánvalóvá vált, hogy a WEP nem nyújt megfelelő védelmet a vezeték nélküli hálózatokat használó eszközök számára. AZ IEEE 802.11i szabványban új biztonsági funkciókat vezettek be. A Wifi-s hálózatoknál alapvető hiba lép fel. Egyrészt a rádiós csatorna jellege miatt a kommunikáció könnyen lehallgatható, másrészt a hálózathoz való csatlakozás nem igényel fizikai hozzáférést a hálózati hozáférési ponthoz, ezért bárki megpróbálhatja a hálózat szolgáltatásait illegálisan igénybe venni. A WEP az első problémát az üzenetek rejtjelezésével próbálja megoldani, a második probléma megoldása érdekében pedig megköveteli a csatlakozni kívánó eszköz vagy más néven station hitelesítését a hozzáférési pont felé. A hitelesítést egy egyszerű kihívás-válasz alapú protokoll végzi, amely négy üzenet cseréjéből áll. Elsőként a station jelzi, hogy szeretné hitelesíteni magát ez a hitelesítési kérelem. Válaszul a hozzáférési pont generál egy véletlen számot, s azt kihívásként elküldi a stationnak ez a hitelesítés kihívás. A station rejtjelezi a kihívást, s az eredményt visszaküldi, az hozzáférési pontnak ezt nevezik hitelesítési válasznak. A station a rejtjelezést egy olyan titkos kulccsal végzi, amelyet csak a station és a hozzáférési pont ismer. Ezért ha a hozzáférési pont sikeresen visszakódolja a választ, azaz ha a visszakódolás eredményeként visszakapja saját kihívását, akkor elhiszi, hogy a választ az adott station állította elő, hiszen csak az ismeri a helyes válasz generálásához szükséges titkos kulcsot. Miután a hitelesítés megtörtént, a station és a hozzáférési pont üzeneteiket rejtjelezve küldik egymásnak. A rejtjelezéshez ugyanazt a titkos kulcsot használják, mint a hitelesítéshez. A WEP rejtjelező algoritmusa az RC4 kulcsfolyam kódoló. A kulcsfolyam kódolók úgy működnek, hogy egy kisméretű, néhány bájtos titkos kulcsból egy hosszú bájtsorozatot állítanak elő, és ezen sorozat bájtjait XOR-olják az üzenet bájtjaihoz. A XOR gyakorlatilag a kizáró vagy aritmetikai logikai egység. Ez történik a WEP esetében is. Az M üzenet küldője a titkos kulccsal inicializálja az RC4 kódolót, majd az RC4 által előállított K bájtsorozatot XOR-olja az üzenethez. Az MK rejtjelezett üzenet vevője ugyanazt teszi, mint a küldő, a titkos kulccsal inicializálja az RC4 algoritmust, amely így ugyanazt a K bájtsorozatot állítja elő, amit a rejtjelezéshez használt a küldő. Látható, hogy ha a rejtjelezés a fentiek szerint működne, akkor minden üzenethez

ugyanazt a K bájtsorozatot XOR-olnánk, hiszen a kódolót minden üzenet elküldése előtt ugyanazzal a titkos kulccsal inicializáljuk. Ha egy támadó lehallgatja a két rejtjelezett üzenetet XOR-olva a támadó a két nyílt üzenet XOR összegét kapja. Ez olyan, mintha az egyik üzenetet a másik üzenettel, mint kulcsfolyammal rejtjeleztük volna. Valójában az M1 M2 egy nagyon gyenge rejtjelezés, és a támadó az üzenetek statisztikai tulajdonságait felhasználva könnyen meg tudja fejteni mindkét üzenetet. Az is előfordulhat, hogy a támadó részlegesen ismeri az egyik üzenet tartalmát, és annak segítségével a másik üzenet tartalmához hozzájut. A problémák elkerülése érdekében, a WEP nem egyszerűen a titkos kulcsot használja a rejtjelezéshez, hanem azt kiegészíti egy inicializáló vektorral, amely üzenetenként változik. Az inicializáló vektort és a titkos kulcsot összefűzzük, a kapott értékkel inicializáljuk az RC4 kódolót, mely előállítja az bájtsorozatot, amit az üzenethez XOR-olunk. A vevőnek szüksége van a kódolásnál használt vektorra Ez a rejtjelezett üzenethez fűzve, nyíltan kerül átvitelre. Az inicializáló vektor 24 bites, a titkos kulcs pedig 104 bites. A rejtjelezés előtt, a küldő egy integritás-védő ellenőrző összeggel egészíti ki a nyílt üzenetet, amelynek célja a szándékos módosítások detektálásának lehetővé tétele a vevő számára. A WEP esetében az ellenőrző összeg a nyílt üzenetre számolt CRC érték. A CRC önmagában nem véd a szándékos módosítások ellen ezért a WEP a CRC értéket is rejtjelezi. A szábvány lehetővé teszi, hogy minden station-nak saját titkos kulcsa legyen, amit csak a hozzáférési ponttal oszt meg. Ez azonban megnehezíti a kulcsmenedzsmentet a hozzáférési pont oldalán, mivel ekkor a hozzáférési pontnak minden station kulcsát ismernie kell. A legtöbb implementáció nem támogatja ezt a lehetőséget. A szabvány előír egy úgynevezett default kulcsot, amit a hozzáférési pont és a hálózathoz tartozó minden eszköz ismer. A kulcsot azon üzenetek védelmére szánták, melyeket a hozzáférési pontok többes szórással (broadcast) minden vezeték nélküli eszköznek el szeretne küldeni. A legtöbb WEP implementáció azonban csak ezt a megoldást támogatja. Így a gyakorlatban, egy adott hálózathoz tartozó eszközök egyetlen közös kulcsot használnak titkos kulcsként. Ezt a kulcsot manuálisan kell telepíteni az eszközökben és a hozzáférési pontokban. Ez a megoldás csak egy külső támadó ellen biztosítja a kommunikáció biztonságát.

Hitelesítési hibák

A WEP-nek van pár hibája, gyakorlatilag a kitűzött biztonsági célok közül egyet sem valósít meg tökéletesen. A WEP hitelesítési eljárásának több problémája is van. Elsőként az,

hogy a hitelesítés egyirányú, azaz a station hitelesíti magát a hozzáférési pont felé, ám a hozzáférési pont nem hitelesíti magát a station felé. Második probléma, hogy a hitelesítés és a rejtjelezés ugyanazzal a titkos kulccsal történik. Ez azért nem jó, mert így a támadó mind a hitelesítési, mind pedig a rejtjelezési eljárás potenciális gyengeségeit kihasználhatja egy, a titkos kulcs megfejtésére irányuló támadásban. Biztonságosabb lenne, ha minden funkcióhoz külön kulcs tartozna. A harmadik problémája a WEP-nek, hogy a protokoll csak a hálózathoz történő csatlakozáskor hitelesíti a stationt. Amikor a hitelesítés megtörtént és a station csatlakozott a hálózathoz, bárki küldhet a station nevében üzeneteket annak a MAC címét használva. Ez azért lehet nagy probléma, mert az összes station egy közös titkos kulcsot használ, és így a támadó megteheti azt, hogy az egyik eszköz által küldött és közben a támadó által lehallgatott üzenetet egy másik eszköz nevében megismétel a hozzáférési pont felé, és ezt a hozzáférési pont fogja fogadni. A WEP rejtjelezési algoritmusa az RC4 folyamkódoló. Nemcsak az üzeneteket kódolják az RC4 segítségével, hanem a station ezt használja a hitelesítés során is a hozzáférési pont által küldött kihívás rejtjelezésére, ez a negyedik hiba. A gyakorlatban minden, az adott hálózathoz tartozó eszköz ugyanazt a titkos kulcsot használja, a támadó ezek után bármelyik eszköz nevében csatlakozni tud a hálózathoz. Persze a csatlakozás még nem elegendő, a támadó használni is szeretné a hálózatot. Ehhez olyan üzeneteket kell fabrikálnia, amit a hozzáférési pont elfogad. A hitelesítésekben ez a négy fő probléma van a WEP titkosítással kapcsolatban.

Titkosítási hibák

A WEP szabványnál azonban még hibák jelennek meg a titkosítás során. A probléma abból adódik, hogy az inicializáló vektor csak 24 bites, ami azt jelenti, hogy körülbelül 17 millió lehetséges inicializáló vektor van. Egy WiFi eszköz körülbelül ötszáz teljes hosszúságú keretet tud forgalmazni egy másodperc alatt, így a teljes vektor teret 7 óra alatt kimeríti. Azaz 7 óránként ismétlődnek az inicializáló vektor értékek, és ezzel az RC4 által előállított bájtsorozatok is. A problémát súlyosbítja, hogy a minden eszköz ugyanazt a titkos kulcsot használja, különböző vektor értékekkel, így ha egyszerre n eszköz használja a hálózatot, akkor az inicializáló vektor ütközés várható ideje a 7 óra n-ed részére csökken. Egy másik fő probléma, hogy sok WEP implementáció az inicializáló vektort nem véletlen értékről indítja, hanem nulláról. Ezért beindítás után a különböző eszközök ugyanazt a nullától induló és egyesével növekvő vektor sorozatot használják. A támadónak várakoznia sem kell, azonnal

vektorütközésekhez jut. Az RC4 kódoló rossz használata a WEP teljes összeomlását okoza. Ha valaki meg tudja figyelni egy gyenge kulcsból előállított bájtsorozat első néhány bájtját, akkor abból következtetni tud a kulcsra.

5.2.2 WPA[28]

A WPA a Wireless Protected Access rövidítése. A WPA a WEP hiányosságait és hibáit hivatott kiküszöbölni, a vezeték nélküli rendszerek egy a WEP-nél biztonságosabb protokollja. A 802.11i szabvány elődjének tekinthető amelyet egy ipari csoport definiált, amely úgy lett kialakítva, hogy együttműködjön az összes vezeték nélküli hálózati eszközzel, de az első generációs eszközökkel nem minden esetben kompatibilis. A WPA a 802.1X hitelesítési protokolljait egészíti ki és az adat sértetlenségének megőrzésére a WEP-el szemben több titkosítási algoritmust is használ. A WPA által igényelt egyetlen titkosítás a ideiglenes kulcs integritási protokoll TKIP (TKIP, Temporary Key Integrity Protocol), amely a WEP által az integritás ellenőrzésére és a bejutások észlelésére és azok reagálására szánt alap RC4 titkosítást bővíti ki. A régebbi hardverek esetében csak szoftveres módosítással tehető működőképessé a TKIP. A WPA tartalmaz még egy úgynevezett AES-CCMP titkosítást is. Ez a specifikáció WPA2-ként ismert. A WPA előír titkosítási és hitelesítési protokollokat. A hitelesítés általában a 802.11X vagy egy háttérszolgáltatás alapján történik, például RADIUS segítségével, vagy egy előre megosztott kulcsot alkalmazó minimális kézfogással a station és a hozzáférési pont között, Az elsőt WPA Enterprise-nak a másodikat WPA Personal-nak hívják. általánosságban a vezeték nélküli hálózatoknál nem használnak RADIUS alapú szervert, ehelyett WPA-PSK-t használnak.

PSK

A WPA-PSK, vagyis a WPA-Personal, egy adott jelszó alapján generált előre megosztott kulcssal (pre-shared key, PSK) működik, amit a vezeték nélküli hálózatokban mesterkulcsként használnak. Minden egyes vezeték nélküli felhasználó azonos kulcson osztozik. A WPA-PSK olyan kisméretű vezeték nélküli hálózatok esetében megfelelő, ahol a hitelesítést elvégző szerver használata nem lehetséges.

[28] Chris Hurley és tsi (szerk) - How to Cheat at Securing a Wireless Network, Syngress Publishing (2006)

EAP-TLS

A másik mód, a 802.1X hitelesítési szerveren keresztül történik, és ebben az esetben WPA-Enterprise-ról van szó. Ez sokkal biztonságosabb a WPA-Personal előre kiosztott kulcsaival szemben. A WPA-Enterprise a bővíthető hitelesítési protokoll (EAP, Extensible Authentication Protocol) használatán alapszik. Az EAP önmaga nem végez titkosítást, mivel úgy alakították ki, hogy magát az EAP protokollt kell egy titkosított járaton keresztül bújtatni. Az EAP hitelesítési módszereinek több típusát is kidolgozták, melyek közül a legismertebbek az EAP-TLS, EAP-TTLS valamint az EAP-PEAP. Az EAP-TLS a vezeték nélküli hálózatokon egy nagyon jól támogatott hitelesítési protokoll, mivel ez volt az első EAP módszer, amit a WiFi szövetség jóváhagyott. Az EAP-TLS működéséhez három tanúsítvány kell, egy hitelesítő hatóságtól (Certificate Authority, CA), egy a hitelesítést végző szervertől és egy a klienstől. Ezzel az EAP módszerrel mind a hitelesítő szerver, mind a vezeték nélküli kliens külön képviselik a saját tanúsítványaikat.

EAP-TTLS

Az EAP-TTLS a szállítási rétegbeli védelmet jelenti. Az EAP-TLS használatakor mind a hitelesítést végző hozzáférési pontnak és station-nak is kell tanúsítvány, azonban az EAP-TTLS esetében a stantion-nál ez elhagyható. Ez a módszer nagyjából olyan, mint amit a webes oldalak csinálnak, ahol a web szerverek egy védett SSL tunnelt képeznek még akkor is, amikor a látogatók nem rendelkeznek kliens oldali tanúsítvánnyal. Az EAP-TTLS egy titkosított TLS tunnelen keresztül védi le a hitelesítési adatok forgalmát.

EAP-PEAP

A PEAP gyakorlatilag védett EAP. Az EAP-TTLS egyik alternatívájaként jött létre. A PEAP módszernek két változata van, amelyek közül az egyik a PEAPv0/EAP-MSCHAPv2. A PEAP az EAP-TLS után a leginkább alkalmazott szabvány, ha a hálózatunkban többféle operációs rendszer is megtalálható, akkor az EAP-TLS után valószínűleg a PEAP lesz a másik, amit mindegyik ismerni fog. A PEAP hasonló az EAP-TTLS-hez, szerver oldali tanúsítványokkal hitelesíti a klienseket és titkosított TLS tunnelt hoz létre a kliens és a hitelesítést végző szerver között. Biztonság szempontjából az EAP-TTLS és a PEAP között az a különbség, hogy a PEAP hitelesítés a felhasználói nevet titkosítatlanul küldi el és csak a

jelszó megy át a titkosított TLS tunnelen. Az EAP-TTLS egyaránt a TLS tunnelt használja mind a felhasználói név, mind a jelszó esetében.

5.2.3 WPA2

A WiFis eszközök biztonságát növelő funkciók következő szintje a WPA2. Ez az IEEE 802.11i szabványra épül. Új titkosítási és biztonsági eljárásaival nagyobb biztonságot nyújt, mint a WEP vagy a WPA.Az alapvető különbség a WPA és a WPA2 között az alkalmazott titkosítási algoritmus, a WPA esetén RC4/TKIP, a WPA2-nél pedig a robusztusabb AES-CCMP. Az AES-CCMP algoritmus felel meg egyedül a legmagasabb szintű biztonságot megkövetelő számítógépes biztonságának. Nem minden eszköz alkalmazásnál indokolt a WPA2 használata, elsősorban a nagyon magas szintű adatvédelmi igény esetén érdemes bevezetni. A vezeték nélküli eszköz kezdeményezi a cellaváltást, ami szigorú titkosítási algoritmusok esetén egy gyors azonosítást és új kulcs kiosztását jelenti. A WPA2 egyébként egy erősebb vállalati szabványt és egy kisebb teljesítményű személyes-WPA2 algoritmust takar. Utóbbi otthoni használatra javasolt elsősorban, mivel előre kiosztott kulccsal dolgozik a rendszer. A vállalati felhasználásra szánt WPA2 változat autentikációs szervertől kapja a kulcsokat, ilyen például az AAA/RADIUS szerver. A WPA2 visszafelé kompatibilis a WPA-val, így egy rendszerben egyszerre mindkét titkosítási módszer használható. Ez elsősorban az antennákra vonatkozik, amelyek többfajta mobil egységet is ki tudnak szolgálni egy időben, eltérő titkosítás alkalmazásával. A 802.11i és a WPA2 között az alapvető különbséget a barangolás gyorsaságában érzékelhetjük, így azokban a rendszerekben, ahol beszéd vagy mozgókép átvitele történik, a 802.11i támogatás elengedhetetlen, mivel a WPA2 ezt a fajta gyorsaságot nem biztosítja teljes körűen. A Microsoft Windows XP WPA2 támogatása hivatalosan 2005. május 1-jétıl kezdve létezik. A meghajtó-programok frissítése szükséges lehet. Az Apple támogatja a WPA2-t az összes AirPort Extreme Macintoshban, az AirPort Extreme Base Station-ökben, és a AirPort Expressz-ekben. A szükséges Firmwarefrissítést tartalmazza az AirPort 4.2, 2005. július 14-én kibocsátott változata.

5.2.4 TKIP és AES-CCMP[29]

A **Temporal Key Integrity Protocol** jelentése időszakos kulcs sérthetetlenségi protokoll. Az IEE 802.11 szabványban található meg biztonsági protokolként. A TKIP a WiFi szövetség szerint az egyik lehetőség a WEP kiváltására, a már meglévő vezeték nélküli eszközök lecserélésének szükségessége nélkül. A TKIP a WEP-hez képest három biztonsági funkciót valósít meg, az egyik a kulcsösszekeverés, ami a titkos gyökér kulcsot összekeveri az inicializáló vektorral, még az előtt, hogy eljutna az RC4 inicializáláshoz. Míg a WEP csak összefűzte az inicializáló vektort a gyökér kulccsal és továbbította az RC4 algoritmusnak. A második biztonsági elem, a WPA végrehajt egy fokozatos számlálást az ismétlődő támadások kivédésére, a csomagokat, amiket üzemen kívül kapott meg, el fogja utasítani a hozzáférési pont. A harmadik biztonsági funkciója a TKIP-nek, hogy végrehajt egy 64 bites üzenet sértetlenségi vizsgálatot, amit MICHAEL-nek hívnak. A Michael állomás szinten működik, azaz a felsőbb protokollszintről a MAC szintre érkező adatokon, fragmentálás előtt végzi az integritás-védő ellenőrző összeg számítását, ami lehetővé teszi a hálózati kártya meghajtó programjában történő megvalósítást. Ez azért fontos, mert így a Michael bevezetése egyszerű szoftver upgrade-del megoldható. A TKIP egy kisebb frissítéssel képes futni a régebbi WEP-es eszközökön, az RC4 algoritmust kihasználva. Az üzenet sérthetetlenségének vizsgálata megakadályozza a hamisított csomagok elfogadását. A TKIP egy kulcs folyam (keystream) visszaállító támadás által sebezhető. Ha sikerül eredményesen végrehajtani a keystream-et, akkor megengedi a támadónak, hogy átküldjön hét és tizenöt darab csomagot a hálózaton. Az aktuális, nyilvánosan elérhető TKIP specifikus támadások nem fedik fel a páros mester kulcsot (Pairwise Master Key) vagy a páros időszakos kulcsokat (Pairwise Temporal Keys).

TKIP titkosítás

A WEP titkosítás legfőbb hibáját az inicializáló vektor kis mérete és a gyenge RC4 kulcsok használata jelentette. A TKIP-ben ezért az inicializáló vektor méretét 24 bitről megnövelték 48 bitre. Ez egyszerű megoldásnak látszik, ám a nehézséget az okozza, hogy a WEP-et támogató hardverek adott hosszúságú 128 bites értékkel inicializálják az RC4 algoritmust, s így a megnövelt inicializáló vektort, a rejtjelező kulccsal együtt, valamilyen

[29] Elkészítéshez a Wireless Security - The Newnes Know It All Series (2009) könyvet és a http://www.technet.hu/forum/ fórumot használtam.

módon „bele kell gyömöszölni” ebbe az adott hosszúságba. A gyenge kulcsok problémáját a TKIP úgy oldja meg, hogy minden üzenet rejtjelezését más kulccsal végzi. Így a támadó nem tud a sikeres támadáshoz szükséges számú, azonos kulccsal kódolt üzenetet megfigyelni. Az üzenetkulcsokat a TKIP a négy utas kézfogás során generált adat-rejtjelező kulcsból állítja elő.

Az **Advanced Encryption Standard - Counter CBC-MAC Protocol** rövidítésneve AES-CCMP. Ez a vezeték nélküli adatátvitel védelmének új, az IEEE 802.11i szabvány szerinti módszere. Az AES-CCMP erősebb titkosítást biztosít, mint a TKIP. Az AES-CCMP tervezőinek bizonyos értelemben könnyebb dolguk volt, mint a TKIP tervezőinek, hiszen nem volt megkötés arra vonatkozóan, hogy a protokollnak milyen hardveren kell futnia. A tervezők ezért egyszerűen megszabadultak az RC4 algoritmustól, s helyette az AES blokkrejtjelezőre építették fel a protokollt. Definiáltak egy új AES használati módot, mely a régóta ismert CTR (Counter) mód és a CBC-MAC (Cipher Block Chaining – Message Authentication Code) kombinációja. Ebből származik a CCMP rövidítés. CCMP módban, az üzenet küldője először kiszámolja az üzenet CBCMAC értékét, ezt az üzenethez csatolja, majd az üzenetet CTR módban rejtjelezi. A CBC-MAC számítás kiterjed az üzenet fejlécére is, a rejtjelezés azonban csak az üzenet hasznos tartalmára és a CBC-MAC értékre vonatkozik. A CCMP mód tehát egyszerre biztosítja a teljes üzenet (beleértve a fejlécet is) integritásának védelmét és az üzenet tartalmának titkosságát. A visszajátszás ellen az üzenetek sorszámozásával védekezik a protokoll. A sorszám a CBC-MAC számításhoz szükséges inicializáló blokkban van elhelyezve.

5.2.5 Hitelesítés és hozzáférés[30]

A 802.1X modell három résztvevőt különböztet meg a hitelesítés folyamatában: a hitelesítendő felet (supplicant), a hitelesítőt (authenticator), és a hitelesítő szervert (authentication server). A hitelesítendő fél szeretne a hálózat szolgáltatásaihoz hozzáférni, és ennek érdekében szeretné magát hitelesíteni, azaz kilétét bizonyítani. A hitelesítő kontrollálja a hálózathoz történő hozzáférést. A modellben ez úgy történik, hogy a hitelesítő egy úgynevezett port állapotát vezérli. Alapállapotban a porton adatforgalom nincs engedélyezve, ám sikeres hitelesítés esetén a hitelesítő „bekapcsolja” a portot, ezzel engedélyezve a

[30] Chris Hurley és tsi (szerk) - Wardriving and Wireless Penetration Testing, Syngress Publishing (2006)

hitelesítendő fél adatforgalmát a porton keresztül. A hitelesítő szerver az engedélyező szerepet játssza. Tulajdonképpen a hitelesítendő fél hitelesítését nem a hitelesítő, hanem a hitelesítő szerver végzi, és ha a hitelesítés sikeres volt, engedélyezi, hogy a hitelesítő bekapcsolja a portot. WiFi hálózatok esetében a hitelesítendő fél az eszköz, mely szeretne a hálózathoz csatlakozni, a hitelesítő pedig a hozzáférési pont, amely a hálózathoz történő hozzáférést kontrollálja. A hitelesítő szerver egy program, mely kisebb hálózatok esetében akár a hozzáférési pontban is futhat, nagyobb hálózatoknál azonban tipikusan egy külön erre a célra dedikált hoszton futó szerveralkalmazás. WiFi esetében a port nem egy fizikai csatlakozó, hanem egy logikai csatlakozási pont, amit a hozzáférési pontban futó szoftver valósít meg. Maga a hitelesítés az EAP segítségével történik. Az EAP csak egy illesztő-protokoll, amit arra terveztek, hogy tetszőleges hitelesítő protokoll üzeneteit szállítani tudja. Egy adott hitelesítő protokoll EAP-ba történő beágyazásának szabályait külön kell specifikálni. Több elterjedt hitelesítő protokollra létezik már ilyen specifikáció. Négy fajta EAP üzenet létezik: request, response, success, és failure. Az EAP request és response üzenetek szállítják a beágyazott hitelesítő protokoll üzeneteit. Az EAP success és failure speciális üzenetek, melyek segítségével a hitelesítés eredményét lehet jelezni a hitelesítendő fél felé.

5.3 Feltöréshez használt eszközök

Az az ember, aki tényleg kiszemelt magának egy feltörni kívánt hálózatot, és ha még rendelkezik egy haladó szintű informatikai tudással, akkor nem kell hozzá hatalmas tudásanyag, hogy bárki feltörjön egy otthoni vezeték nélküli hálózatot.

5.3.1 Szoftverek az interneten

Az interneten rengeteg olyan szoftvert lehet találni, amely segítségével fel lehet törni WiFi-s hálózatokat, főleg akkor, ha kicsit még utána is néz az ember a webes oldlak között egy program működési leírásért. Több oldalas részletes szöveges leírásokat lehet találni WiFi-s titkosítások feltöréséről, több internetes fórum is foglalkozik ezekkel a témákkal, amelyek azért is lehetnek fokozottan veszélyesek, mert azok a felhasználók, akik egyáltalán nem értenek hozzá, hogy hogyan kell esetleg egy feltörő programot használni, és a különböző leírásokban nem igazodna el, akkor a fórum többi felhasználójától tud segítséget kérni.

Azonban található több videó megosztó portálon előre rögzített képsorozatok, amelyek bemutatják, képi segédlettel, hogy hogyan is kell egy titkosított WiFi-s hálózatot feltörni.

5.2.2 Fizikai eszközök

Egy vezeték nélküli hálózat feltöréséhez a megfelelő szoftverek beszerzése egyszerű, majdnem olyan egyszerű a megfelelő fizikai eszközök beszerzése is. Csupán egy olyan vezeték nélküli hálózati eszközre van szükségünk, mely képes csatlakozni hozzáférési pontokhoz, és támogatja az IEEE 802.11a/b/g/n szabványokat. Ilyen eszközök lehetnek olyan hálózati kártyák, melyek vezeték nélküli kacsoltra képesek, ezek lehetnek USB-n keresztül csatlakoztatottak, vagy laptopba, számítógépe beszereltek. Lehet kapni különböző antennákat, erősítőket, melyekkel növelni lehet egy támadó eszköz hatótávolságát. Ezeket az eszközöket pár ezer forintból be lehet szerezni, szinte bármelyik informatikai boltba, ebből láthatjuk, hogy WiFi-s hálózataink nagy veszélynek vannak kitéve, legyen szó céges, vagy egyszerű hálózatokról.

6 A puding próbája

6.1 Tesztelt hálózat elemei

Ebben a fejezetben bemutatom, hogy mennyire védtelen lehet otthoni vezeték nélküli hálózatunk. Az otthoni hálózatomból készítettem egy teszthálózatot, hogy azért mégse más hálózatára lépjek be illetéktelenül.

A hálózat routerből és két laptopból áll. A router egy D-link 802.11g/2,4Ghz-es ISM sávon üzemelő hozzáférési pont. Az egyik laptop erre a hozzáférési pontra van csatlakoztatva, mint egyszerű felhasználói eszköz, a másik laptoppal pedig az illetéktelen behatolót szimuláltam.A támadó gépen egy Mixrosoft Windows 7 64 bites verziója futott, ezen a gépen egy CommView for WiFi 6.3-as verzió számú szoftver és egy Aircrak-ng 1.1 csomagot használtam a teszt hálózatra való betöréshez. A felhasználói laptopon egy Microsoft Windows7 futott.

A célom az volt a teszt hálózat felállításával, és feltörésével, hogy megnézzem, mennyi idő alatt lehet bejutni egy hálózatba, és ott milyen adatokhoz juthat hozzá egy illetéktelen betolakodó.

6.2 Támadások lépései

A támadó laptopra feltettem egy Aircrack-n 1.1 verzió számú programot. Az aircrack egy wireless auditing tool, mellyel a wireless hálózatok biztonsága tesztelhető, de akár fel is törhető. Ez az egyik legprofesszionálisabb programcsomag mely a dinamikus fejlesztése mellett több platformon is elérhető Windows és Linux operációs rendszereken is. A program fő funkciói csak az általa támogatott vezeték nélküli hálózati eszközök használata esetén lehetséges. A tesztben Windows XP alatt mutatom be az Aircrack programmal egy hálózat feltörését, azonban Linux operációs rendszereknél nagyobb az Aircrack hálózati kártya támogatása, mivel ott több hálózati kártya használható úgynevezett injectációra. Injectációnak nevezzük, amikor egy hálózati forgalomba csomagokat szúrunk be, forgatunk vissza.

Elhelyezése a számítógépes eszközön igen egyszerű Windows esetében, még telepítésre sincs szükségünk, egyszerűen csak a Google segítségével igen hamar rátalálunk, letöltjük egy tömörített formátumban, és csak ki kell csomagolnunk számítógépünkre. Ezek mellett telepítettem a támadó laptopra egy CommView for WiFi 6.3-as verzió számú szoftver, mely a monitorozásban és a hálózatok scannelésében volt segítségemre.

6.2.1 Aircrack-ng csomag[31]

Az Aircrack-ban is található erre egy úgynevezett Airmon-ng, amely segítségével monitor módba tehetjük a hálózati interfészünket, így lehetőségünk nyílik a hálózat monitorozására, scannelésére. Azonban támadó gépen nem működött ez a funkciója az Aircrack-nek, ezért a CommonView for WiFi programmal végeztem a hálózati kártya monitor módba való kapcsolását, a hálózatok monitorozását és csomagok elkapását.

[31] Chris Hurley és tsi (szerk) Wardriving and Wireless Penetration Testing Syngress Publishing (2006)

Az Aircrack csomag része még az airodump-ng is. Az airodump-ng segítségével scannelhetjük a WiFi hálózatokat a már monitor módba léptetett hálózati interfészünkkel. Az airodump-ng segítségével megnézhetjük:

- A WiFi router MAC címét/ BSSID
- Jelerősséget dBm -ben (-50 dBm a legerősebb)/ Power
- A hozzáférési pont által küldött ébrenléti csomagok, ezek alapján hirdeti magát/ Beacons
- A wireless router által küldött adat csomagok számát/ Data
- A hozzáférési pont csatorna számát/ Channel
- Mennyi a hozzáférési pont által küldött csomagok száma másodpercenként
- A hozzáférési pont által támogatott maximális adatátviteli sebességet/ MB
- A titkosítás típusát határozza (WEP/ WPA/WPA2)/ ENC
- A titkosítás algoritmusát (TKIP/CCMP/Mixed)/ Cipher
- A vezeték nélküli hálózat nevét/ ESSID

Ahogy láthatjuk, ha egy támadó eszköz egy vezeték nélküli hálózat hatósugarán belül tartózkodik, akkor minden lényeges adatot meglehet tudni, egy ingyenes letöltető csomag segítségével, ezért is fontos, hogy minél biztonságosabban állítsuk be hálózatunkat

. Megtalálható az Aricrack csomagban egy aireplay-ng is. Az aireplay-ng segítségével csomagokat injectálhatunk vagy forgathatunk vissza a hálózatba, ehhez csupán egy olyan hálózati eszközre és az eszközhöz driverre van szükségünk, amely támogatja ezt. Az airplay-ng-vel lehetőségünk nyílik:

- A hozzáférési pont és a csatlakozó eszköz közötti kapcsolat megszakítására.
- Hamis authetnikációt lehet létrehozni a hozzáférési ponttal.
- Egy lementett cap fájl alapján képes a fájlban lévő csomagokat visszaforgatni, feltörni kívánt vezeték nélküli hálózatba

- A hozzáférési pont és a vezeték nélküli hálózathoz csatlakozott eszköz közötti ARP kérést elkapni és azt a küldő MAC címével visszaforgatni. Mivel az ARP csomag mérete 28 byte, ebből lehet következtetni arra, hogy titkosított ARP csomagról van e szó.

- Chopchop technikával olyan csomagokat hoz létre, amit ha a WiFi-s hálózatba visszaforgatunk, a router eszköz válaszol, és elegendő csomagot lehet elkapni a WEP kulcs visszafejtéséhez.

- A fregmentációt alkalmazva olyan csomagot hoz létre, amit a Wifi-s hálózatba visszaforgatva az router válaszol, és elegendő csomagot tudunk elkapni a WEP kulcs visszafejtéséhez.

- A vezeték nélkülihálózathoz csatlakozott felhasználói eszköz felé történő kérés az inicializáló vektorkért.

- Injectációs tesztet lehet végrehajtani vele.

Összességében az Aircrack-ng feladata, a jelszó visszafejtése egy fájlból, melyet lementettünk korábban. Az Aircrack két fajtat töréshez használható a WEP titkosítás feltöréséhez, és a fejlettebb WPA és WPA2 titkosítás feltöréséhez. Egy egyszerűbb WEP titkosítás feltöréséhez több megoldás létezik. Megpróbálhatjuk statisztikai úton visszafejteni a kulcsokat, akkor el kell kapni a feltörni kívánt hálózatból n mennyiségű DATA csomagot. Ha a WEP 64 bites titkosítást alkalmaz, akkor körübellül 10000 DATA csomag elkapása szükséges, míg ha már erősebb 128 bites titkosítás van a feltörni kívánt hálózaton, akkor körübellül 20000 és 40000 közötti DATA csomag elkapása szükséges. Ezek a tikosítás komolyságától és a jelszóban használt karakterek milyenségétől számít. A másik feltörési mód a szótárfájl alapú törés, WEP kulcsok esetében ez is működik. Ekkor egy szótárfájl elérését meg kell adni a visszafejtési próbálkozás előtt. Általában WEP titkosítás visszafejtéséhez a statisztika támadást használják, mert nagyon gyors, pár perc alatt elvégezhető, és ha megvan a DATA csomag kellő mennyisége, akkor 100%-os a pontosság.

6.2.2 WPA/WPA2 feltörési lehetőségek

Ha WPA vagy WPA2 titkosítással ellátott WiFi-s hálózatot próbálnánk feltörni, akkor csak szótár alapú feltörés működik. Ennél a támadási formánál nem csak a lementett

csomagokat, de egy szótárfájl is meg kell adni. A lementett csomagok útvonala és a szótárfájl útvonal megadása után a feltörő program visszafejti a kódot. A szótárfájlok gyakorlatilag csak szavakat tartalmaznak, sokat segíthet, ha a szótárfájlban csoportosítva vannak témakörök szerint a lehetséges jelszavak. Például ha a feltörni kívánt hálózat tulajdonosáról tudjuk, hogy szereti a kanadai jégkorongot, és van egy olyan csoportosítás a szótárfájlban, hogy sportok és azon belül Kanada, akkor nagyobb hatékonysággal használható a szótárfájlos feltörés WPA és WPA2 titkosítású hálózatoknál. Azonban ennél a módszernél nem garantált az, hogy sikeres lesz a feltörési próbálkozás végeredménye.

A WPA és WPA2 titkosítású hálózatok feltörésére van egy másik módszer, ami hatékonyabb a szótárfájlosnál, a brute force eljárás. Ez az eljárás gyakorlatilag az mint a szótárfájlos, sok lehetséges jelszót próbálnak össze, és amelyik jó lehet, azt felajánlják a végén mint lehetséges jó jelszó. Azonban lassú, folyamat, és egy ElcomSoft nevű informatikai biztonsággal foglalkozó orosz cég egy olyan feltörő eszközt adott ki, mely az előbb említett brute force eljárásra épül, és azt nagyban felgyorsítja, ezt jelszó-visszaállítónak nevezték el. Az eszköz több párhuzamos szálat indít a titkosítás feltörésére, de nem a számítógép processzorát használja, hanem a gépek grafikus kártyájának a GPU-ját, melyeket hálózatba kell kötni. A WPA titkosítás feltörés persze így sem egyszerű, jelentős gyorsításhoz ugyanis sok grafikus processzor kell. Azonban ha megfelelő környezet megvan, az ElcomSoft eszközével akár százszor gyorsabban eljuthatunk az eredményhez, mint a hagyományos processzorokkal. Ez azt jelenti, hogy egy év helyett három vagy négy nap alatt megvan az hálózati jelszó. A WAP/WPA2 titkosítás feltöréséhez mindössze néhány adatcsomagra van szükség, tehát a hosszas lehallgatás is megspórolható. Ráadásul a termék a GPU-k tömegét képes ellátni feladattal.

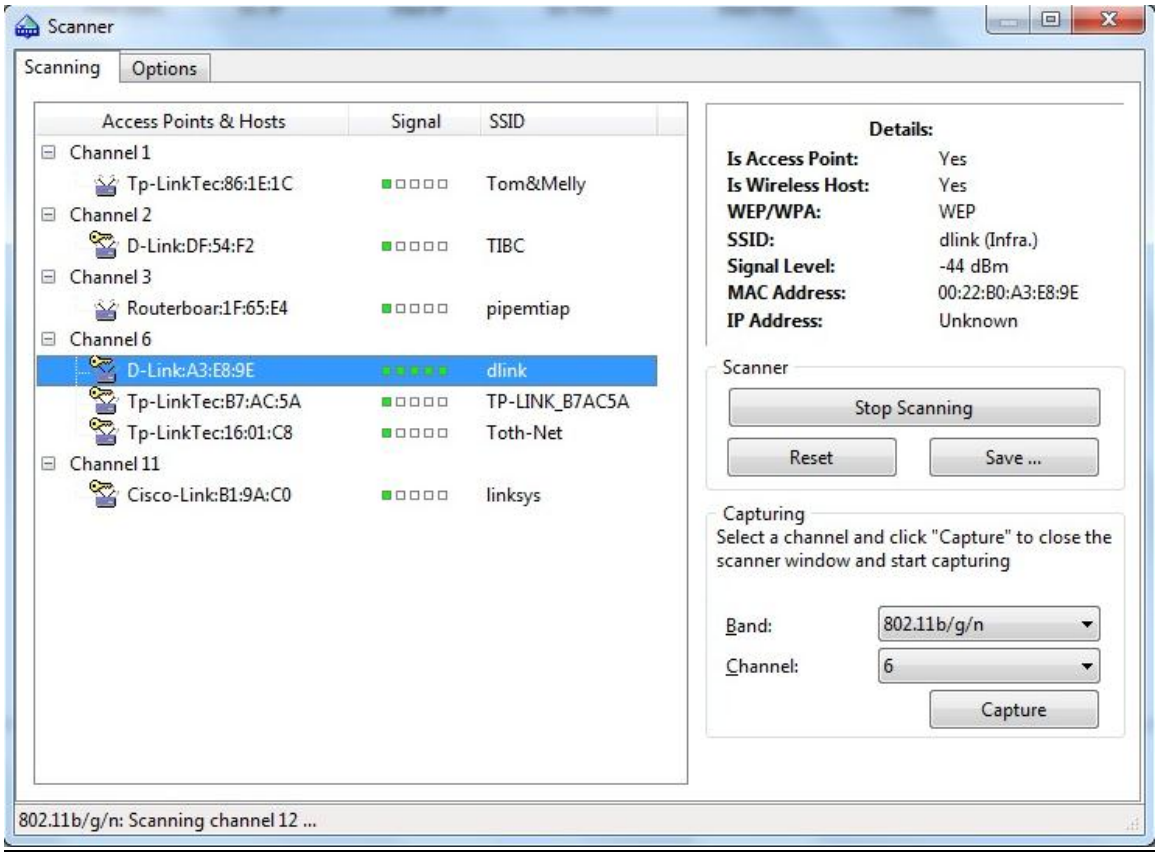
6.2.3 Jelszó megszerzés bemutatása

Korábban már említettem, hogy milyen eszközökből állt a teszt hálózat, amit összeállítottam, és milyen programokat használtam, a feltöréshez. A támadó rendszer készen állt, és telepítve volt a két program (CommView for WiFi és Aircrack-ng csomag). Ezek mellett telepítenem kellett egy drivert, Windows alatt csak atheros csipszettel szerelt hálózati kártyákon mükődik ez az eljárás. A CommView for WiFi első indításakor már fel is ajánlotta, hogy nem rendelkezem a hálózatok monitorozásához megfelelő driverrel, és hogy telepítem,

hogy a hálózati kártya megfelelő legyen, a CommView For Wifi-ben való hálózat felderítéshez, monitorozáshoz.

A CommView For Wifi programot, ha elindítjuk, akkor monitorozó üzemmódba váltja a hálózati kártyánkat, ha esetleg WiFi-n keresztül csatlakozva voltunk idáig egy hálózatra, akkor ez meg is szakadt. A programban egy két beállítás nem árt, hogy csomagokat mekkora méretben mentse le a program, a lementés helyét és a nevét a fájlnak, a könnyebb visszakeresés érdekébe. Miután ezekkel megvoltam, elindítottam a Scanner funkciót, amely segítségével felderítettem a közelben lévő vezeték nélküli hálózatokat.

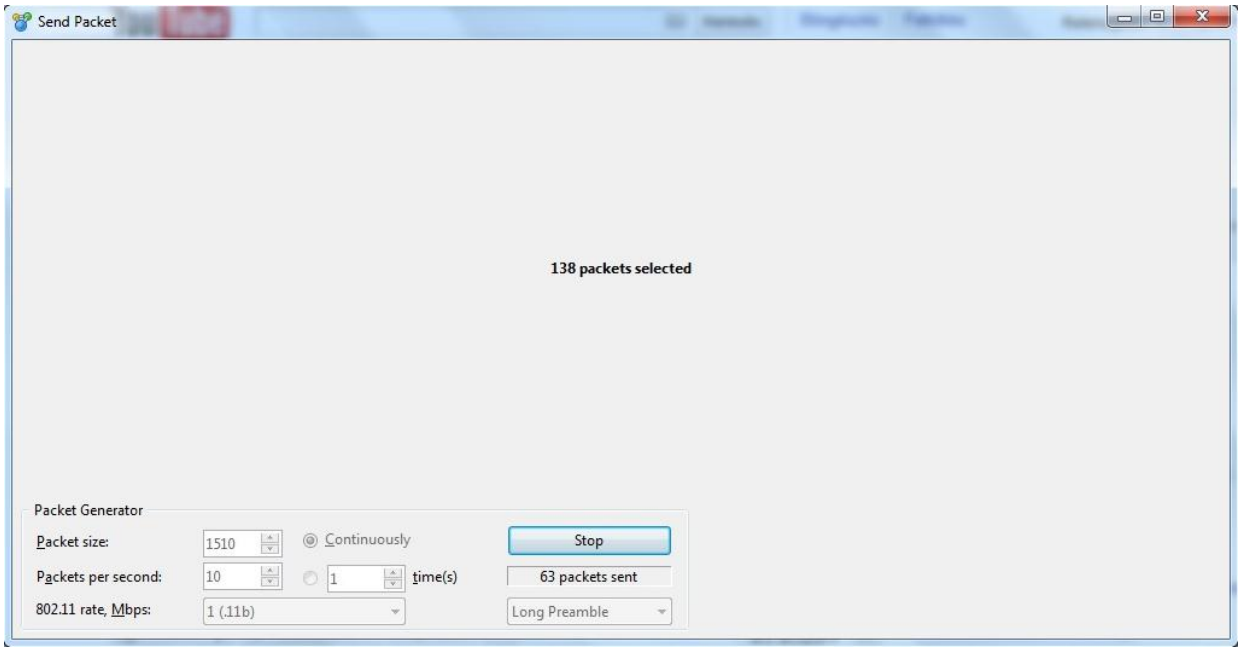
*CommView for WiFi program szkennelés közben **3.** ábra*



A hálózat felderítés után a 3. ábrán látható vezeték nélküli hálózatok hatókörzetében helyezkedtem el a támadásra felszerelt laptoppal. Már a monitorozás során rengeteg adatot meglehet tudni egy adott hálózatról, például, a MAC címét, a titkosítás típusát, a jel erősségét. Miután felderítettem a hálózatokat, kiválasztottam azt a tesztelésre beállított hálózatot, hogy

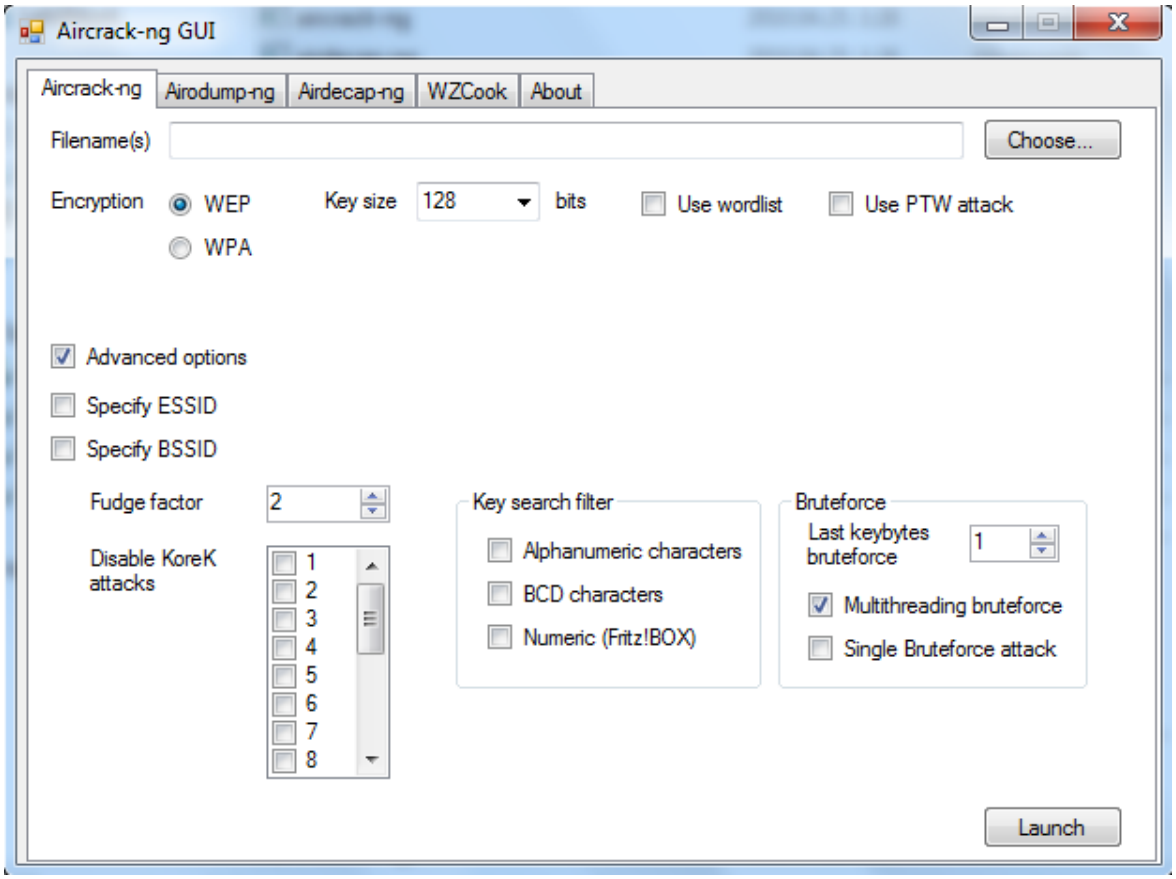
annak a hálózatnak kezdje el figyelni a csomagjait. Ezek után a tesztelésre beállított hálózatnak elkezdtem visszaküldeni csomagokat, a CommView For Wifi program sand packet funkciójával.

*CommView for WiFi program Send Packet funkció **4.** ábra*



Van egy számláló, mely mutatja, hogy hány csomagot sikerült elfogni a programmal, és ha körülbelül elértük a WEP titkosításnál a 10000-ret, akkor biztosan állhatunk neki a titkosított jelszó visszafejtéshez. Ehhez meg kell nyitnunk a CommView for WiFi által lementett csomagok fájlját, és egy .CAP formátumban kell lementenünk. Azért kell ilyen formátumba elmenteni a fájlt, mert az Aircrack-ng csomag, ilyen formátumban tudja megnyitni a lementett csomagokat. Az Aircrack-ng csomag megnyitása után be kell meg kell adnunk az útvonalát a lementett .CAP kiterjesztésű fájlnak, amely a csomagokat tartalmazza.

*Aircrack-ng csomag **5.** ábra*



Miután megadtam az elérési útvonalát a .CAP állománynak, el is kezdtem a Launch gombra kattintva elindítottam a kód visszafejtési eljárást. Először az Aircrack-ng csomag betöltötte a .CAP állományból csomagokat, és parancssoros felületen felsorakoztatta az elkapott csomagokat, inicializáló vektor szerint csökkenő sorrendbe. Gyakorlatilag az a hálózat került a legfelülre, amelyiket a CommView for Wifi programban kiválasztottunk monitorozásra. Azonban nem csak a figyelésre kiválasztott teszt hálózat titkosítási szintjét és MAC címét láthatjuk, hanem az összes olyan hálózatét is, amelynek a hatókörzetében elhelyezkedünk a támadásra beállított eszközzel. Végezetül ki választottam azt a hálózatot, amit eredetileg is tesztelés szempontjából beállítottam, és az Aircrack-ng csomagban található visszafejtő algoritmussal sikeresen visszafejtettem a teszthálózatnál korábban megadott jelszótitkosítást.

6.3 Biztonságos WiFi hálózat beállítása

6.3.1 Megfelelő hely választása

Az egyik legfontosabb feladatunk, hogy megfelelő helyen helyezzük el hozzáférési pontunkat, ez azért nagyon fontos, mert ezzel csökkenthetjük a lehetőségét annak, hogy valaki benne legyen a hozzáférési pontunk hatótávolságában. Többnyire úgy kell elhelyezni a hozzáférési pontot, hogy gondoljuk, végig hol szeretnénk, használni a vezeték nélküli lehetőségeket, és ezek a pontok még benne legyenek az Access Point hatótávolságában, de az utcáról, szomszédból ne nagyon nyíljon lehetőség arra, hogy bárki rácsatlakozhasson hálózatunkra. Sokan esnek abba a hibába, hogy nem törődnek a hozzáférési pont megfelelő elhelyezésével, hanem oda telepítik az eszközt, ahova az internet is közvetlenül be van kötve. Ez a folyamat lehet, hogy úgy tűnik, hogy nem fontos, de ha sikerül azt a hatótávolságot elérni, hogy csak házunkon belül és udvarunkon legyen látható a vezeték nélküli hálózatunk jele, akkor nagy mértékben lejjebb csökkentjük a hálózatunkat látó külső hozzáférők számát.

6.3.2 SSID megválasztása[32]

Az SSID a Service Set Identifier rövidítése, ami szolgáltatás névazonosítást jelent. Az SSID a vezeték nélküli hálózatok esetében használt azonosító, melyet az adatcsomagokhoz kapcsolnak. Ez alapján lehet azonosítani, hogy az adatcsomagok, mely hálózathoz tartoznak. Ezen felül az SSID egy hálózati eszközcsoport azonosítására is szolgál, annak érdekében, hogy az adatkapcsolat a különböző WLAN eszközök, azaz az állomások és hozzáférési pont között létrejöjjön, ugyanazzal a SSID beállítására van szükség. Természetesen beállíthatjuk, a SSID-t, hogy könnyebben tudjuk azonosítani a hálózatunkat, 32 karakter hosszú lehet maximálisan az azonosító, az azonosító lehet például *linksys, dlink, otthoni wlan*. Maga az azonosító szöveges és alfa numerikus karakterekből állhat. Ajánlott használni a SSID Broadcast-et, amely arra szolgál, hogy láthatatlanná teszi hálózatunkat, miután beállítottuk megfelelően a hálózatunkat, akkor ajánlott a SSID-t kikapcsolni, a vezeték nélküli eszközök, amiket korábban csatlakoztattunk a hálózatra, azok továbbra is tudnak majd csatlakozni, de akik később próbálnánk, azok nem látják majd a hálózatunkat, ezáltal nem is tudnak majd róla.

[32] Chris Hurley és tsi (szerk) How to Cheat at Securing a Wireless Network, Syngress Publishing (2006)

6.3.3 AP és Router jelszava

A hozzáférési pont és a router jelszavak megváltása gyakorlatilag az adminisztrátori jelszó, aki ismeri a felhasználó nevet és a jelszót, az be tud lépni AP vagy routerünkre. Ez a beállítás is igen fontos, mivel a biztonságot növeli, általában mindig gyári beállításon hagyják a felhasználók. Ha egy támadó sikeresen belép hálózatunkra, és gyári beállításokon hagytuk jelszavunkat, felhasználói nevünket, akkor igen egyszerűen be tudnak lépni hálózatunk központi egységébe, és át tudják állítani azt. A gyártók többnyire minden egyes eszköznél, amit kiadnak ugyan azt az adminisztrátori nevet és jelszót használják, sok esetben jelszót nem is adnak meg. Például a Cisco és D-Link eszközök „admin" felhasználói nevet alkalmaznak, jelszót többnyire nem, de ezeket felhasználói kézikönyvekből vagy az interneten pár perces keresgélés után megtalálhatóak, ezek az alapértelmezett adminisztrátori nevek.

6.3.4 MAC address

A MAC *(Media Access Control)* egy hexadecimális számsorozat, amellyel még a gyártás során látják el a hálózati eszközöket. Belépve egy routerbe van arra lehetőség, hogy mivel minden hálózati eszköznek saját MAC címe van, megadhatjuk, hogy kik léphessenek csak be hálózatunkra. A hackerek tudnak MAC címet hamísítani, lemásolni, és esetleg be tudnának lépni hálózatunkra, úgy hogy korábban lemásolták egyik eszközünk hálózati MAC címét, és a saját eszközükét arra állítják be, de az egyszerű próbálkozók ellen ez a beállítás még mindig védelmet biztosít. Ezt a beállítási lehetőséget úgy kell felfogni, hogy privát belépési lehetőséget adunk azoknak, akiket szeretnénk, hogy használják hálózatunkat, akik nincsenek benne ebben a listában, azok nem léphetnek be. A MAC címek szűrésének akkor lehet nagy hátránya, hogyha olyan helyen alkalmazzuk, ahol sok vezeték nélküli eszköz fordul meg, mert ebben az esetben minden egyes alkalommal, amikor egy új eszköz számára szeretnénk internet és hálózat hozzáférést biztosítani, akkor be kell lépnünk az AP, vagy router eszközbe és a MAC cím szűrőlistához hozzáadni a kívánt eszköz azonosítóját. Azonban ez a módszer olyan kis otthoni és céges hálózatoknál tökéletes, ahol minden nap ugyan azokat az eszközöket alkalmazzuk csak.

6.3.5 Titkosítás használata

A legfontosabb egy hálózat védelme érdekében, a megfelelő titkosítás megválasztása. A WEP titkosítást nem ajánlom, mert pár perc alatt fel lehett törni, bizonyítottan kis védelmet

biztosít, és rengeteg hibája van amit a feltörő programok kihasználnak és így könnyedén juthatunk be WEP titkosítással védett hálózatokra. A WPA már fejlettebb titkosítás, de azt is több idő és több energia ráfordításával fel lehet törni. Akinek lehetősége van WPA2 titkosítást alkalmazni, akkor az azt használja. WPA2 titkosítást használó hálózatokra, csak nagy rutinra és hozzáértésre szert tett hackerek tudnak belépni sikeresen. Manapság ez a titkosítási mód ami megfelelő védelmet nyújthat WiFi-s hálózatunk számára.

6.3.6 IP cím beállítás

Egy lehetőség van, amit érdemes megemlíteni, amely növelheti a WLAN hálózatok biztonságát, az pedig a routerek által kioszható IP címek tartománya és száma az eszközök száma. Többnyire a routerek IP címét is alapértelmezettként hagyják az emberek, amely például lehet *192.168.0.1* vagy *192.168.2.* ezeket sem árt megváltoztatni, bármilyen értékeket megadhatunk, mert ez a router által a belső hálózat felé kiosztott IP címek lesznek. Kifelé nem ezt az IP címet fogják látni az Access Pointok, hanem az internet szolgáltatónk által adott IP címet, vagyis ha ezt a címet átállítjuk nem lesz belőle semmi gond. Ezeket a számokat 0 és 255 intervallum között adhatjuk meg. A másik IP címmekkel kapcsolatos beállíátsi lehetőség a kiosztásuk, általában gyári beállításként a routerek DHCP-t alkalmaznak. A DHCP Dynamic Host Configuration Protocol, amely az IP címek automatikus szétosztásáért felelős protokol. Ha csatlakozik egy új eszköz a hálózathoz, akkor az az eszköz egy előre megadott IP tartomány közül olyan címet fog kapni, amely nincs lefoglalva. Lefoglava úgy lehet egy cím, hogy már azt egy másik eszköz, amely a hálózatra csatlakozott már használja. A DHCP nagyon hasznos olyan hálózatok esetében, ahol napi szinten rengeteg új eszköz csatlakozhat a hálózathoz, de kisebb olyan hálózatoknál, amelyeknél általában azonos eszközöket használnak naponta, ott nem árt, ha statikusan (vagyis saját magunk) adjuk meg a hálózati eszközökhöz az IP címeket.

7. Összefoglalás

Szakdolgozatom célja az volt, hogy megmutassa, hogy a vezeték nélküli hálózatok, mennyivel támadhatóbbak, a vezetékes hálózatokkal szemben. A vezetékes hálózatoknál már a hozzáférésnél problémába ütközhetnek azok a személyek, akik megpróbálnának privát hálózatunkba betörni, de a vezeték nélküli hálózatoknál ez a probléma kisebb gond az illetéktelen behatolók szempontjából.

A témát olyan oldalról közelítettem meg, hogy milyen lehetséges megoldások vannak a védelemre, és ezeket a védelmi mechanizmusokat hogyan lehet kihasználni. Azonban ha kellő időt és odafigyelést szánunk a megfelelő védelem kialakítására, akkor biztonságossá tehetjük vezeték nélküli hálózatunkat annyira, hogy ne férhessenek hozzá internetünkhöz és személyes anyagainkhoz, melyek a hálózathoz csatlakozott eszközeinken megtalálhatóak.

Szakdolgozatomat elején leírást készítettem a vezeték nélküli hálózatok kialakulásáról, és a hálózatok típusáról. Említést teszek a WLAN hálózatok mellett megjelent és folyamatosan fejlődő egyéb vezeték nélküli hálózatokról, mint például a mobil internetről, és ami talán most fog a mobil eszközöknek köszönhetően elterjedni NFC-ről. A 802.11 szabvány fejlődéséről is írtam részletesebben, emellett a fő cél az volt, hogy a WLAN hálózatok biztonságáról készítsek részletesebb leírást.

Bemutattam pár lehetséges támadási módot, egy példán keresztül be is mutattam egyet és emellett a biztonságot növelő eszközökre, és azok hasznos használatáról is írtam.

8. Irodalomjegyzék

Könyvek

Chris Hurley és tsi (szerk) - How to Cheat at Securing a Wireless Network, Syngress Publishing (2006)

Chris Hurley és tsi (szerk) - Wardriving and Wireless Penetration Testing, Syngress Publishing (2006)

Jim Geier - Implementing 802.1X Security Solutions for Wired and Wireless Networks, Wiley Publishing (2008)

Jim Geier - Vezeték nélküli hálózatok, PANEM KFT. (2005)

Wireless Security - The Newnes Know It All Series (2009)

Internetes források

Ebookz.hu - A hálózatokról általában. Letöltéve: 2011.02.03

http://ebookz.hu/ebook.php?azon=a04a10

Mobilarena.hu - NFC - a kis hatótávolságú kommunikáció. Letöltve: 2011.04.26.

http://mobilarena.hu/teszt/nfc/mi_az_az_nfc.html

Mobilarena.hu - Adatkommunikációs alapozó. Letöltve: 2011.01.17

http://mobilarena.hu/teszt/adatkommunikacios_alapozo/gprs_edge.html

Internetes oldalak és fórumok:

http://prohardver.hu/index.html

http://www.wxpee.hu/index.php?showtopic=676

http://techline.hu/

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

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

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

http://www.airdefense.net/index.php