SZAKDOLGOZAT

Kéri Balázs Mátyás

Debrecen
2009

Debreceni Egyetem
Informatikai Kar
Informatikai Rendszerek
és Hálózatok Tanszék

Wi-Fi®:
A VEZETÉK NÉLKÜLI SZABADSÁGGAL JÁRÓ PROBLÉMÁK ÁTFOGÓ VIZSGÁLATA

Témavezető:
Dr. Almási Béla
egyetemi docens

Készítette:
Kéri Balázs Mátyás
mérnök informatikus

Debrecen
2009

Tartalomjegyzék:

1. Bevezetés

A legtöbb ember úgy azonosítja be a Wi-Fi kifejezést, mint a képességet, amivel internetezni tudunk vezeték nélkül. Ez a meghatározás nem teljesen fedi a valóságot, a Wi-Fi technológia sokkal többet jelent, mint puszta internetezés. 10 évvel ezelőtt senki sem gondolta volna, hogy lehetséges lesz zenét hallgatni az emeleti számítógépről a nappali hangrendszerén, zenét letölteni a Wi-Fi képes MP3 lejátszónkra, kézi játék konzolunkon több barátunkkal hálózatban játszani, vagy például internetezni a kedvenc kávézónkban.

A Wi-Fi nem csak ezt, hanem még temérdek sok más dolgot tesz számunkra lehetővé, azonban ahhoz, hogy ez mind működjön, és ne legyenek a technológia használásának káros következményei, nagyon sok tényező optimális együttállására van szükség.

A szakdolgozat ezeket a tényezőket veszi górcső alá:
Bemutatja a Wi-Fi technológia fizikai működését, a fizikai megvalósításból származó problémákat, és azok kiküszöbölését. Ismerteti a Wi-Fi technológia fejlődését és az ezzel fellépő kompatibilitási gondokat.
Nagy hangsúlyt fektet a biztonsági kérdésekre, mivel a Wi-Fi-nek vezeték nélküli megvalósításából kifolyólag nagyon komplex biztonsági problémákkal kell szembenéznie.
Nap mint nap emberek százezrei vállnak élő céltáblává, amikor Wi-Fi technológiát támogató eszközeikkel csatlakoznak az Internethez. Ezért a szakdolgozat részletesen kitér a jelenleg elterjedt titkosítási mechanizmusokra, mennyire nyújtanak „valós” védelmet a külső támadásokkal szemben, illetve, hogy ezek hiányában mire számíthatunk.
Az utolsó fejezetben a szakdolgozat bemutat egy, a való világból vett példát. Milyen konkrét veszélyekkel találkozhatunk, ha végigkövetjük egy távmunkás általános napját.
Ha a Wi-Fi technológiát a napunk során többször, több helyen is használjuk, milyen veszélyek leselkednek ránk, még ha tudatában sem vagyunk azoknak.

2. Mi is az a Wi-Fi?

(Forrás: Jim Geier - Vezeték nélküli hálózatok 2005)

A Wi-Fi a Wi-Fi Alliance(Wi-Fi Szövetség) védjegye, mellyel a IEEE 802.11-es szabványra épülő hitelesített termékeket jelölik.

2.1. Története

A Wi-Fi kétféle rádiós technológiát használ:
- single carrier: közvetlen sorozatú szórt spektrum (Direct Sequence Spread Spectrum, DSSS)
- multi carrier: ortogonális frekvencia osztásos multiplexelés (Orthogonal Frequency Division Multiplexing, OFDM)

A szabadon elérhető, nem licenszelt szórt spektrum korábbi szabványai (HomeRF, Bluetooth) tették lehetővé a Wi-Fi kifejlesztését.
A nem licenszelt szórt spektrum tartományai:
902-928 MHz, 2400-2483.5 MHz, 5725-5850 MHz

A nem licenszelt szórt spektrumot elsőnek az FCC (Federal Communications Commission) 1985. május 9-én elfogadott szabályzata tette elérhetővé az USA-ban. Később ezt a szabályzatot fogadták el apróbb módosításokkal minden nagyobb országban.
Az FCC-től a javaslatot Michael Marcus tette 1980-ban, melyet egy 5 éves elfogadási procedúra követte. A kérés egy nagyobb javaslat része volt, melyben a civilek számára elérhetővé akarták tenni a szórt spektrumú technológiát.

Az Wi-Fi elődjét 1991-ben az NCR Corporation/AT&T (később Lucent Technologies & Agere Systems) találta fel Nieuwegein-ben, Hollandiában. Eredetileg pénztárrendszerekhez tervezték, és az első termékeket WaveLAN néven hozták a piacra 1-2 Mbit/s sebességgel. Vic Hayes aki 10 évig volt az IEEE 802.11 elnöke és akit a Wi-Fi „atyjának" neveztek részt vett az IEEE 802.11b, és 802.11a szabványok megtervezésében.

A 802.11 Wi-Fi technológia eredeti szabadalmi jogai a CSIRO-hoz (Australia's Commonwealth Scientific and Industrial Research Organisation) tartoznak. Ezek a szabadalmi jogok voltak a tárgyai a CSIRO és a fő IT vállalatok között elhúzódó jogi vitának, mely a nem-fizetett jogdíjjakról szólt. 2009-ben sikerült megállapodnia a CSIRO-nak 14 vállalattal köztük: Hewlett-Packard, Intel, Dell, Toshiba, ASUS, Microsoft, Nintendo, azzal a feltétellel, hogy a megállapodás részletei nem látnak napvilágot…

2.2. Wi-Fi Alliance

A Wi-Fi Alliance szabványokat támogat azért, hogy az IEEE 802.11-re épülő hálózati eszközök együttműködését javítsa. A Wi-Fi Alliance különálló és független cégek konzorciuma, amely egyetért egy sor szokásos, egymással együttműködő hálózati termékben, amelyek a IEEE 802.11-es szabványra épülnek. A Wi-Fi Alliance termékeket hitelesít meghatározott teszt eljárásokkal. Azok, akik tagjai a Wi-Fi Alliance-nek és átmennek a teszteken, tehetik rá a Wi-Fi logót a termékükre.

2.3. Elnevezés

A Wi-Fi kifejezés Wireless Fidelity-re utal (Vezetéknélküli Pontosság), hasonlóan a rég megalkotott Hi-Fi-hez (High Fidelity). A Wi-Fi önmagában nem jelent semmit, de gyakran a Wi-Fi Alliance maga is ezt az informális kifejezést használja a technológiára hivatkozva.

A Wi-Fi kifejezést kereskedelmileg elsőnek 1999. augusztusában használták, melyet egy márka konzultációs cég (Interbrand Corporation) talált ki, akit a Wi-Fi Alliance azzal bízott meg, hogy találjanak valami „kapósabb" nevet, mint az 'IEEE 802.11b Direct Sequence'.
Az Interbrand találta ki a Hi-Fi szavakkal játszva a Wi-Fi kifejezést, és a yin-yang stílusú logót is.

2.4. Szabványok

Az IEEE 802.11 szabványok csoportja, amely a vezeték nélküli helyi hálózat (WLAN) számítógép-kommunikációját hajtja végre a 2.4, 3.6 és az 5 GHz-es frekvencia tartományokban.

2.4.1. Általános leírás

A 802.11-es család vezeték nélküli modulációs technikákat foglal magába, amik ugyanazt az alap protokollt használják. A legnépszerűbbek a 802.11b és 802.11g által definiált protokollok, amelyek az eredeti szabvány kiegészítései. A 802.11-1997 volt az első vezeték nélküli hálózati szabvány, de a 802.11b volt, amit széles körben el is fogadtak, melyet később a 802.11g és 802.11n követett.
A biztonság eredetileg szándékosan volt gyenge kormányzati beavatkozás (export) következtében, melyet később a kormányzatban és a törvényhozásban történt változások miatt a 802.11i kiegészítésben erősítettek meg.
A 802.11n egy új multi-streamelő modulációs technika.
Más 802.11 szabványok (c–f, h, j…), csak szolgáltatás kiegészítések és módosítások, vagy korábbi specifikációk javításai.

2.4.2. Protokollok

(Forrás: Wikipedia http://en.wikipedia.org/wiki/802.11)

IEEE szabvány	Megjelenés ideje	Működési frekvencia (GHz)	Sebesség (jellemző) (Mbit/s)	Sebesség (maximális) (Mbit/s)	Hatótávolság beltéren (méter)	Hatótávolság kültéren (méter)
Eredeti 802.11	1997	2,4	1	2	~20	~100
802.11a	1999	5	23	54	~35	~120
802.11b	1999	2,4	4,3	11	~38	~140
802.11g	2003	2,4	19	54	~38	~140
802.11n	2009	2,4 / 5	74	600(MIMO)	~70	~250

802.11-1997 (802.11 régi)

A 802.11-es szabvány eredeti verziója 1997-ben jelent meg és 1999-ben hagyták jóvá, de mára ez már teljesen elavult.

Tartalma:

- két hálózati bitráta, 1 és 2 Mbit/s sebességgel
- továbbítási hibajavító kód
- 3 alternatív fizikai rétegbeli technológia:
    - szórt infravörös 1Mbit/s sebességgel
    - frekvenciaugrásos szórt spektrum 1 és 2 Mbit/s sebességgel
    - közvetlen sorozatú szórt spektrum 1 és 2 Mbit/s sebességgel

  Az utóbbi kettő rádiós technológia mikrohullámú átvitelt használt az Industrial Scientific Medical(ISM) frekvencián, 2.4 GHz-en.

802.11b

A 802.11b maximális átviteli sebessége 11 Mbit/s és ugyanazt a közeg-hozzáférési módot használja, mint ami az eredeti szabványban van megadva.

A 802.11b termékek 2000 elején jelentek meg a piacon, mivel a 802.11b közvetlen kiegészítése az eredeti szabványban definiált modulációs technikának.

A drasztikus sebességnövekedés (az eredeti szabványhoz viszonyítva) és a lényeges árcsökkenés vezettek a 802.11b gyors elterjedéséhez, mint meghatározó vezeték nélküli LAN technológia.

A 802.11b eszközök interferencia gondokkal küszködnek a többi, 2.4GHz-en működő eszközöktől: mikrohullámú sütők, Bluetooth eszközök, baba megfigyelők, vezeték nélküli telefonok.

802.11g

2003 júniusában egy harmadik modulációs technikát is jóváhagytak, ez volt a 802.11g.
A 802.11b-hez hasonlóan ez is 2.4GHz-en működik, de ugyanazt az OFDM-en alapuló átviteli sémát használja, mint a 802.11a.

Jellemzői:

- 54 Mbit/s maximális sebesség a fizikai rétegben
- Továbbítási hibajavító kód
- 22 Mbit/s átlagos átviteli sebesség
- Teljesen visszafele kompatibilis, így a 802.11b eszközökkel is együtt tud működni

A 802.11g termékek 2003. januárjában kezdtek megjelenni, jóval a szabvány elfogadása előtt, mivel hatalmas volt az igény a gyorsabb sebességre, és az alacsonyabb előállítási költségre.
2003. nyarára a kétsávos (802.11a/b) termékek nagy része háromsávosra cserélődött, támogatva az a/b/g szabványokat, egyetlen mobil adapter vagy access point formájában.
Ahhoz, hogy b és g hálózatok együtt tudjanak működni, hosszas technikai folyamatok kellenek, ezért egy g-s hálózatban tartózkodó b-s eszköz lelassíthatja az egész hálózat teljesítményét.
A b-hez hasonlóan a g-s eszközök is interferencia gondokkal küszködnek a többi, 2.4GHz-en működő eszközöktől.

802.11g WLAN Router

802.11n

Az IEEE 802.11n a korábbi 802.11-es szabványokra épül, új kiegészítésekkel: többszörös input-többszörös output (multiple-input multiple-output MIMO), 40 MHz-es csatornák a fizikai rétegben, frame aggregáció a MAC rétegben. A MIMO egy technológia, ami több antennát használ, hogy összevetve több információt tudjon visszafejteni, mint egy antennával lenne lehetséges. A MIMO technológia másik képessége az SDM (Spatial Division Multiplexing – Tér Osztásos Multiplexelés). Az SDM több független adatfolyamot multiplex-szel össze a térben, egyetlen adott sávszélességű csatornán belül. A MIMO SDM jelentősen képes megnövelni az átviteli sebességet, ahogy a visszafejtett tér adatfolyamok száma nő. Minden egyes tér adatfolyamhoz szükség van egy önálló antennára mind az adó, mind a vevő oldalon. Továbbá, a MIMO-nak elkülönített rádió frekvencia láncra, és analóg-digitális konverterre van szüksége minden egyes antennához.

A 40 MHz-es csatornaszélesség is egy másik jellemvonása a 802.11n-nek, ami a korábbi 20 MHz-es csatornaszélesség megduplázódása a fizikai rétegben. 5 GHz-en is lehet használni, illetve 2.4 GHz-en feltéve, hogy nem interferál az ugyanazt a frekvenciát használó másik 802.11 illetve nem 802.11 eszközzel.

802.11n WLAN Router

Adatkódolás

Az adó és a vevő elő- és utókódolási technikákat alkalmaz úgy, hogy a MIMO kapcsolatban rejlő kapacitását elérje. Előkódoláshoz tartozik a tér sugáralakítás és a tér kódolás. A tér sugáralakítás javítja a fogadott jel minőségét a dekódolási fázisban. A térkódolás a térbeli multiplexelés segítségével növeli az átviteli sebességet, valamint a hatótávolságot, a térosztást kihasználva (Alamouti kódolás).

Antennák száma

Az egyidejű adatfolyamok számát a link két oldalán használt antennák száma határozza meg. Azonban egyes eszközök tovább limitálják a tér adatfolyamok számát, amelyek egyedi adatot hordozhatnak. Az **A x B : C** képlet segít beazonosítani az adott eszköz paramétereit. Az első

szám (A) az adó antennák számát, a második szám (B) a vevő antennák számát jelöli. A harmadik szám maximális tér adatfolyamok számát jelöli, amelyet az eszköz használni tud.

Például: 2 x 3 : 2 — 2 adó antenna
3 vevő antenna
2 használható tér adatfolyam

A 802.11n szabványban egészen a 4 x 4 : 4 vannak megemlítve a lehetőségek. A legelterjedtebb konfigurációk a következők:

2 x 2 : 2	2 vevő, 2 adó, 2 téradatfolyam
2 x 3 : 2	2 vevő, 3 adó, 2 téradatfolyam
3 x 3 : 2	3 vevő, 3 adó, 2 téradatfolyam

Mint ahogy a felsorolásból is látszik, mindhárom konfiguráció ugyanakkora sebességre képes, csak a használt antennák számában van eltérés.
Jelenleg a 3 x 3 : 3-as konfiguráció van elterjedőben, aminek nagyobb az átviteli sebessége a plusz adatfolyam következtében.

Teljesítménynövekedés a szabványok előrehaladtával

Adatátviteli sebesség

A 600 Mbit/s-es sebességet csak a maximális 4 tér adatfolyam használatával, és 40 MHz-es csatornaszélességgel lehet elérni. A következő táblázat az átviteli sebességek alakulását, attól függően, hogy mit használunk:

Index	Tér adat-folyamok	Modulációs Technika	Kódolási Ráta	Sebesség			
				20 MHz-es csatorna		40 MHz-es csatorna	
				800ns GI	400ns GI	800ns GI	400ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00
...	...	...	...	...	...	...	...
31	4	64-QAM	5/6	260.00	288.90	540.00	600.00

Frame összecsoportosítás (aggregáció)

A fizikai rétegbeli fejlesztések a 802.11 protokollban található fix költségek miatt nem növelik a user szintű adatátvitel sebességét egy bizonyos ponton túl (jeladási folyamat,

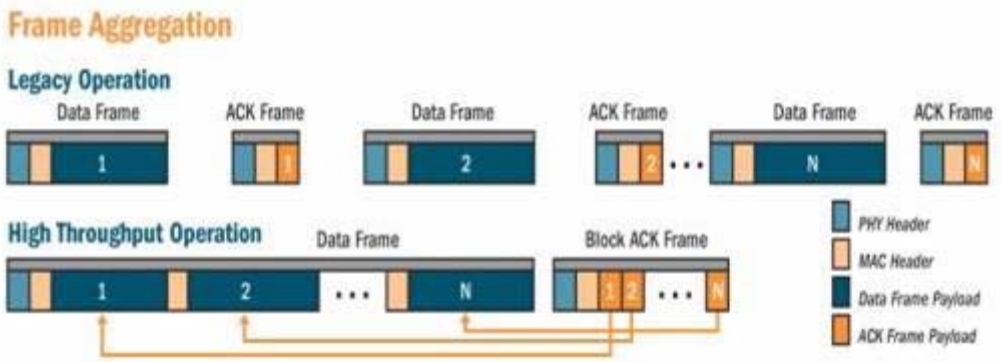
keretküldési időköz, fizikai réteg fejrészei,visszaigazoló framek). A MAC jellegzetessége, ami a teljesítménynövekedést adja, az összecsoportosítás.

Két fajtája van:

1. MSDU-k (MAC Service Data Units) összecsoportosítása a MAC elején (másnéven: MSDU összecsoportosítás, A-MSDU)

2. MPDU-k (MAC Protocol Data Units) összecsoportosítása a MAC végén (másnéven: MPDU összecsoportosítás, A-MPDU)

Az összecsoportosítás egy folyamat, melyben több MSDU-t vagy MPDU-t csomagolunk össze, hogy csökkentsük a fix költségeket, és így növeljük a user szintű adatátvitel sebességét. Az A-MPDU összecsoportosítás használatához szükség van Block visszaigazolásra, ami a 802.11e-ben jelent meg elsőnek és a 802.11n-ben optimizálták.



Visszafele kompatibilitás

Amikor a 802.11g megjelent, hogy megossza a hullámsávot a korábbi 802.11b eszközökkel, módokat biztosított arra, hogy a korábbi és az új eszközök együtt-élése rendben menjen. A 802.11n még jobban odafigyel az együtt-élésre, hogy megóvja saját adását a korábbi eszközöktől.
Ezek a 802.11g/b/a eszközök. A fizikai rétegbeli védekezési eszközök a következők:

1. Mixed Mode Format védekezés (másnéven: L-SIG TXOP védekezés) Mixed módban az „n” adás „a” vagy „g” formájú adásba van beágyazva. 20 MHz-es adásoknál ez a beágyazás védelmet nyújt az „a” és „g” adásoktól, viszont a „b” eszközöknek továbbra is szüksége van CTS(Clear-To-Send) védelemre.

2. A 40 MHz-es csatornát használó adásoknak, „a” és „g” kliensek jelenlétében CTS védelmet kell használniuk, hogy megvédjék magukat a régi eszközök interferenciájától.

3. Egy későbbi „n” adást meg lehet védeni RTS/CTS(Request to Send / Clear to Send) frame cserét vagy CTS frame adást használva korábbi klienseknél.

Még védelemmel is, hatalmas különbség lehet egy tisztán „n” hálózat sebessége és egy korábbi eszközök jelenlétével működő vegyes hálózat sebessége között. Ez a korábbi b/g hálózat probléma kibővülése.

Telepítési Stratégiák

A maximális sebesség elérése érdekében egy tiszta 802.11n 5GHz-es hálózat a javasolt.
Az 5GHz-es sávnak hatalmas a kapacitása köszönhetően a sok nem-átfedő rádiós csatornáknak és a kevesebb rádiós interferenciának összehasonlítva a 2.4 GHz-es sávval.
Egy tisztán 802.11n hálózat lehet nem praktikus elég sok user számára, mivel jelenleg a b/g eszközök vannak túlnyomórészt elterjedve. Ahhoz, hogy egy egész „n” hálózatot működtessünk, le kell cserélni az összes inkompatibilis hálózati kártyát és laptopot. Rövidtávon lehet jobb megoldás egy b/g/n vegyes hálózat, amíg a 802.11n-es hardver el nem terjed teljesen. Egy vegyes hálózatban az az ideális, ha „b” és „g” forgalmat 2.4 GHz-re, az „n” forgalmat pedig 5 GHz-re tesszük.

Végjáték

A szabványosítási folyamat 2009. szeptemberében véget ért, amikor az IEEE Standards Association elfogadta a végleges 802.11n szabványt.

A nagyobb gyártók már 2006. óta gyártanak előzetes verziókat az „n" szabványból (pre-N, draft n, MIMO-based). Ezek a változatok szinte teljesen megegyeznek az „n" szabvány végleges verziójával. Egy firmware frissítésnek elégnek kell lennie, hogy egy 802.11 Draft N eszközből 802.11n eszköz váljon.

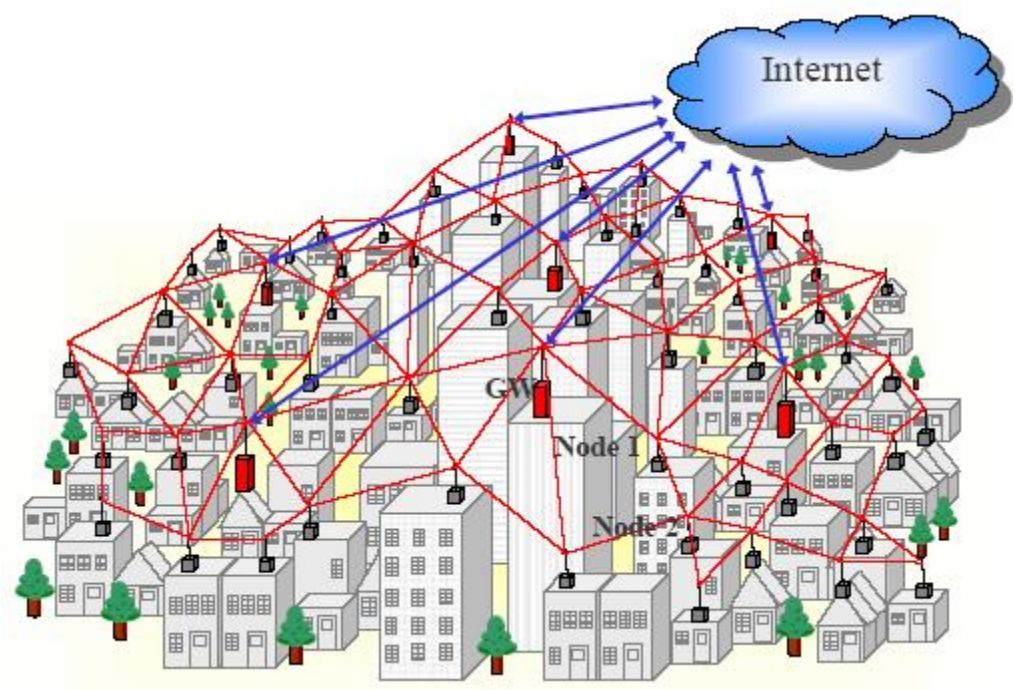
Összehasonlítás:

802.11 szabványok								
802.11 Protokoll	*Kiadás*	*Frekv. (GHz)*	*Sávszél (MHz)*	*Sebesség / stream (Mbit/s)*	*MIMO streamek*	*Moduláció*	*Becsült beltéri hatótáv (m)*	*Becsült kültéri hatótáv (m)*
–	Jún. 1997	2.4	20	1, 2	1	DSSS	20	100
a	Szept. 1999	5 3.7	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	120 5000
b	Szept. 1999	2.4	20	1, 2, 5.5, 11	1	DSSS	38	140
g	Jún. 2003	2.4	20	1, 2, 6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	140
n	Okt. 2009	2.4/5	20	7.2,14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM	~70	~250
			40	15, 30, 45, 60, 90, 120, 135, 150				

2.5. Felhasználási területei

A Wi-Fi technológia napjainkban mindenhol jelen van. Az otthonunkban, vagy munkahelyünkön található Wi-Fi-s eszközök (PC, videójáték konzol, mobiltelefon, PDA, laptop) az internethez és helyi hálózatba kapcsolódnak egy WLAN router (otthoni access point) segítségével. Ez a WLAN router kábel vagy dsl kapcsolaton keresztül átjárót képez az internet felé.

Az access pointok hatósugara a szabványokban leírt távolságig érvényesek, de egymáshoz kapcsolásukkal a lefedett terület mérete az összekapcsolt eszközök számával növelhető. Egy szoba méretétől több négyzetkilométerig terjedhet a lefedettség mértéke. Erre az összekapcsolt hálózatra példa a WMN (Wireless Mesh Network), ahol több egymást átfedő rádiós állomás fedi le az adott területet.



WMN implementáció

Hot Spotok

A védett otthoni és irodai használaton kívül a Wi-Fi Hot Spot-ok segítségével bárki számára elérhetővé válik az internet. Ezeket a Hot Spot-okat vagy ingyenes, vagy ellenérték fejében vehetjük igénybe. Ország szerte több száz regisztrált (www.hotspotter.hu) ingyenesen hozzáférhető Hot Spot áll rendelkezésünkre az Internet elérése, de a később leírtakból kiderül, mire is kell ügyelnünk ilyen helyzetben.

Ad-hoc mód

A Wi-Fi lehetőséget nyújt peer-to-peer kapcsolat létrehozására is, amely lehetővé teszi, hogy az eszközök közvetlenül egymáshoz csatlakozhassanak. Ez az ad-hoc mód közkedveltnek bizonyult multiplayeres kézi videójáték konzolok (Nintendo DS, Iphone), digitális kamerák és más fogyasztói elektronikai cikkek tekintetében. Azonban számos okból (pl. biztonság) kifolyólag ezt a módot nem használják PC-k közti adatátvitelre.

3. Technológiai problémák

(Jim Geier - Vezeték nélküli hálózatok 2005)

3.1. Csatornák

A 802.11 a fentebb említett frekvenciasávokat csatornákra osztja. Például a 2.4000–2.4835 GHz-es sávot 13 csatornára osztja, amelyek egyenként 22 MHz szélesek, a köztük lévő távolság pedig 5 MHz. Az 1. csatorna középpontja 2.412 GHz, a 13.-é 2.472 GHz, amihez még Japán egy 14. csatornát is ad, 12 MHz-cel 13. felett.

A csatornák elérhetőségét az országok maguk szabályozzák, attól függően, hogy a rádiós spektrumot az adott ország, hogyan osztja fel.

Néhány nemzetközi szabályozás:

- Japán mind 14 csatorna használatát engedélyezi kivéve 802.11g/n-nél a 14-est.
- Az európai országok nagy része Japánhoz hasonlóan csak a 14-es csatornát nem engedélyezi.
- Az amerikai kontinensen több ország a 12-es és a 13-as csatornát sem engedélyezi.

Csatorna	Frekvencia (MHz)	Észak Amerika	Japán	A világ többi része
1	2412	Igen	Igen	Igen
2	2417	Igen	Igen	Igen
3	2422	Igen	Igen	Igen
4	2427	Igen	Igen	Igen
5	2432	Igen	Igen	Igen
6	2437	Igen	Igen	Igen
7	2442	Igen	Igen	Igen
8	2447	Igen	Igen	Igen
9	2452	Igen	Igen	Igen
10	2457	Igen	Igen	Igen
11	2462	Igen	Igen	Igen
12	2467	Nem	Igen	Igen
13	2472	Nem	Igen	Igen
14	2484	Nem	Csak „b”	Nem

Amellett, hogy a közép-frekvencia értékét megadja a csatornáknak, a 802.11 megad még egy maszkot, ami meghatározza az energia megengedett eloszlását a csatornák között. A maszk előírja, hogy a jelet 30 dB-lel kell legyengíteni a csúcsértékéhez képest, úgy hogy a csatornák

effektív szélessége 22 MHz legyen. Következésképp az állomások csak minden 4. és 5. csatornát tudnak használni átfedés nélkül.

A gyakorlat:

- USA-ban 1-6-11-es csatornák
- Európában is 1-6-11-es csatornák, habár elméletben 1-5-9-13 is lehetne...

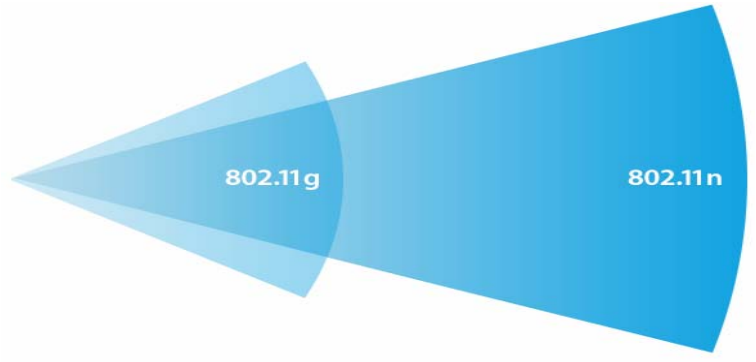
A másik dolog, hogy a csatornáknak 2.401–2.483 GHz-ig kellene tartaniuk, ami a valóságban:

- USA (FCC) 11 Csatorna: 2.412GHz~2.462GHz
- Európa (ETSI) 13 Csatorna: 2.412GHz~2.472GHz
- Japán 13 Csatorna: 2.412GHz~2.472GHz

Ha nem csak ezeket a nem-átfedő csatornákat használjuk, akkor a jel minősége és az átviteli sebesség nagyon leromolhat.

3.2. Hatótávolság és mobilitás

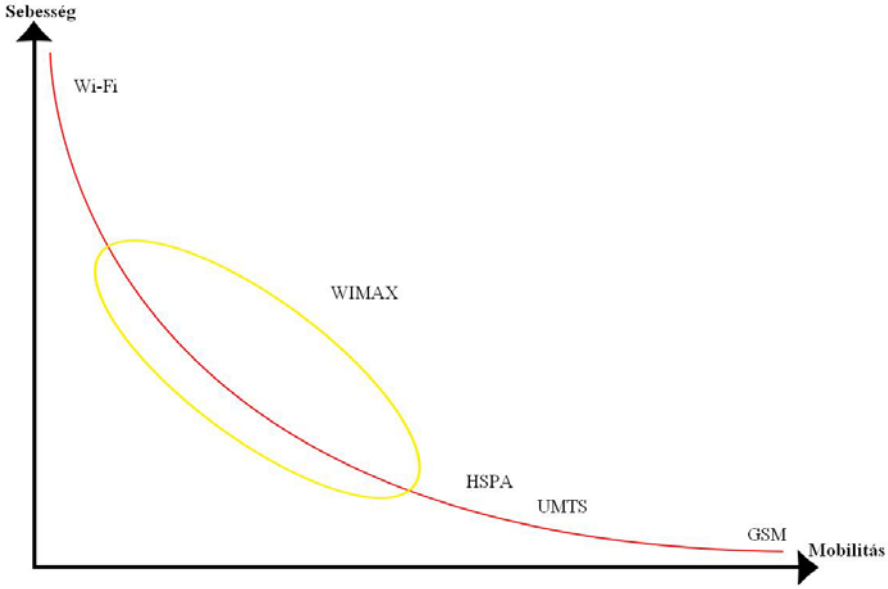
A Wi-Fi hálózatoknak véges hatótávolsága van. Egy tipikus vezeték nélküli routernek 802.11b vagy 802.11g-t használva, gyári antennával beltéren 32 méter, kültéren 95 méter a hatótávolsága. A 802.11n szabvány azonban ezeket a hatótávolságokat megkétszerezi.



A hatótávolság függ a frekvenciasávtól is. A 2.4 GHz-es blokk kicsivel jobb helyzetben van mint az 5 GHz-es. A kültéri hatótávolság irányított antennákkal kilométereket is képes átszelni, természetesen közvetlen rálátással.

A Wi-Fi áramfogyasztása meglehetősen nagy, ezért az akkumlátorok töltöttségi szintje egy elég nagy probléma a mobil eszközöket használók számára.

A Wi-Fi teljesítménye a távolság növekedésével négyzetesen arányosan csökken, valamint a mozgó eszközök tekintetében is, minél gyorsabban mozgunk, annál lassabb az adatátvitel. Más vezeték nélküli technológiák alkalmasabbak az ilyen jellegű feladatokra:



Technológiai összehasonlítás

3.3. ElektroMágneses Interferencia (EMI)

(Forrás: Wikipedia
http://en.wikipedia.org/wiki/Electromagnetic_interference_at_2.4_GHz)

A 2.4 GHz-es tartományt sok eszköz használja, így az elektromágneses interferencia sok gondot okoz a Wi-Fi eszközöknek.

3.3.1. Az interferencia okozói

Vezeték néküli telefonok

Sok vezeték nélküli telefon a 2.4 GHz-es frekvenciát használja, ugyanazt, amelyen a Wi-Fi szabványai, a 802.11b/g/n üzemelnek. Ez jelentős sebességcsökkenést okozhat, vagy teljesen blokkolhatja a Wi-Fi jeleket, amikor a telefont használják.
Néhány példa, hogyan szüntessük meg ezt a problémát:

- használjunk vezetékes telefont,

- használjunk DECT 6.0 (1.9 GHz), 5.8 GHz vagy 900 MHz-en működő telefonokat,
- használjunk VoIP/WiFi telefont,
- teszteljük a különböző csatornákat, hogy elkerüljük a vezeték nélküli telefonok által használtakat

  Ez a teszt nem mindig lesz sikeres, mivel sok vezeték nélküli telefon képes a DSS technológiára. Ez a technológia arra lett tervezve, hogy meggátolja a lehallgatásokat, de ezt használva a telefon a csatornákat véletlenszerűen váltogatja, lehetetlenné téve a Wi-Fi kommunikációt.

Bluetooth

Azért, hogy elkerülje az interferenciát, a bluetooth protokoll úgy van megtervezve, hogy a frekvenciatartományt nem 13, hanem 79 csatornára osztja (egyenként 1 MHz szélesek), és ezek között a csatornák között váltogat másodpercenként 1600-szor. Ez a technika blokkolhatja egy Wi-Fi eszköz teljes kommunikációját, ha elég közel van az eszközhöz.

Autó-riasztók

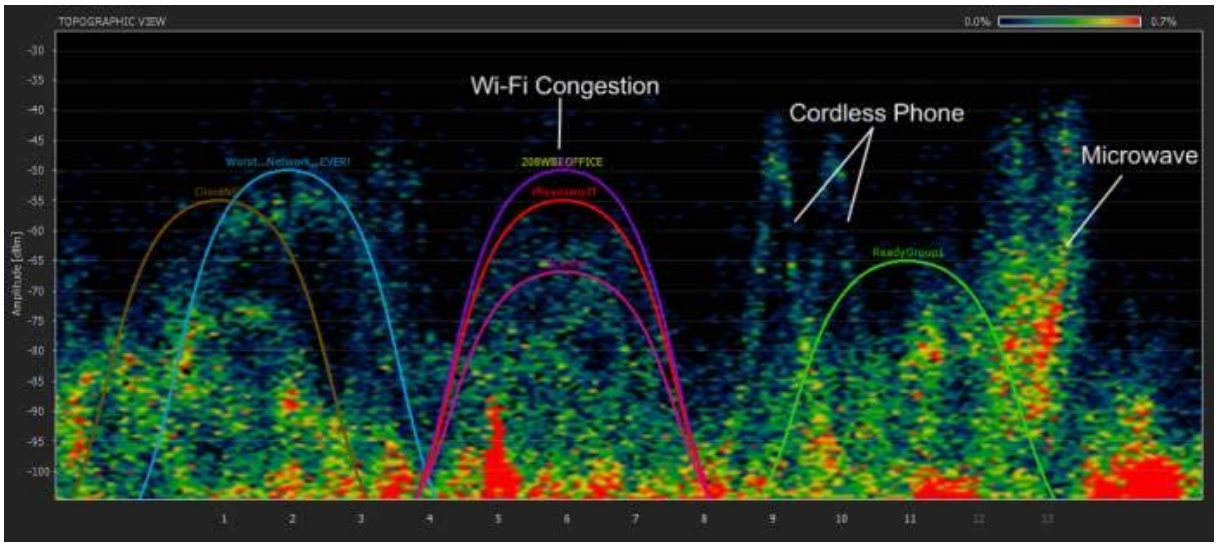
Néhány autógyártó a 2.4 GHz-es frekvenciát használja az autó-riasztóik belső mozgásérzékelőihez. Ezek az érzékelők 2.45 GHz-en (8-as és 9-es csatornák között) sugároznak, 500 mW erősséggel. A csatorna átfedés következtében, ez gondot fog okozni 6-os és 11-es csatornák esetében, amelyek az alapértelmezett csatornák a Wi-Fi kapcsolatoknál. Mivel ez a jel folyamatos, bizonyos problémákat okozhat a Wi-Fi kommunikációban.

Mikrohullámú sütők

A mikrohullámú sütők nagy energiájú jelet bocsátanak ki a 2.4 GHz-es frekvenciasávon. Fontos, hogy ezek a sütők jól árnyékoltak legyenek, mert amúgy erősen zavaró jelet bocsátanak ki. Hatótávolság csökkenést, illetve teljes blokkolást is okozhatnak.

Videó rendszerek

Alaphelyzetben a videójel-továbbító eszközök nagy része alacsony energiával (10mW) sugároznak, de egyes vezeték nélküli kamerák a megengedett érték többszörösével közvetítenek, így zavarva a Wi-Fi kommunikációt.



EMI a 2.4 GHz-es tartományban

3.3.2. Az interferencia gondok kiküszöbölése

Alapesetben nem nehéz megtalálni az interferencia forrását. Veszünk egy usb-s spektrum analizálót, egy laptopot, és felkutatjuk a forrást.

Csatornaváltás

Néha a legegyszerűbb módja, hogy megszüntessük az interferenciát, az hogy átállítjuk a zavaró eszköz által használt csatornát. Ez olyan esetekben könnyű megoldás, ahol a zavaró eszköz könnyen hozzáférhető helyen található, viszont bizonyos esetekben elég nagy problémát tud okozni, például egy komplett megfigyelő rendszer videokameráinak az átállítása.

Jelzavarás

Az interferenciára egyik megoldás a jelzavarás.Jogilag azt tekintve, hogy hogyan is tesszük ezt, szabályos. Egy gyakran használt módszer, ha fogunk egy acces point-ot és az általunk használt (egyéb eszköz által zavart) csatornára állítjuk, a jelerősséget feltoljuk a maximumra, a jeltávolságot pedig 1ms-ra konfiguráljuk. Ez a beállítás a saját 802.11-es hálózatunkban interferenciát fog okozni, viszont kisebbet, mint a zavaró eszköz, mert a CSMA (carrier sense multiple access) ezt minimalizálja. Ez azért hatékony még, mert az így keltett jel a zavaró eszközben szintén interferenciát okoz, meggátolva azt saját, zavaró jelének kibocsátásában. Vannak olyan termékek most is a piacon, amelyek kifejezetten 2.4 GHz-es jelzavarók, amelyeket arra terveztek, hogy megvédjék a 802.11-es hálózatokat más, interferenciát okozó eszközöktől.

Jelzavaró

Alternatív termék

Ismételten az egyik legkézenfekvőbb megoldás, ha kicseréljük a zavaró eszközt, egy olyanra, ami nem zavarja a 802.11-es hálózatunkat (vezetékes kamera, vezetékes telefon), vagy egy olyan eszköz, ami szándékosan másik frekvenciára van gyárilag állítva.

A jelátvitel módjának megváltoztatása

Extrém esetekben, amikor az interferencia szándékos, vagy minden megszüntetésére irányuló kísérlet kudarcot vallott, lehetséges, hogy az antennák típusának megváltoztatása segít. A

kollineráis antennákról nagy teljesítményű, irányított tányér antennákra való áttérés segíthet, mivel a tányér antenna keskeny sugara miatt fizikailag nem is látja (érzékeli) az interferenciát. A szektor antennák esetében kiküszöbölhető az interferencia, ha egy spektrumanalizálót használva megkeressük a zavaró eszközt, és úgy állítjuk be a lefedett területet, hogy ez azon kívül essen.

Bázisállomások hozzáadása

Több bázisállomás hozzáadásával csökkenthető a szomszédos eszközök által okozott interferencia. Minden Wi-Fi szabványban benne van az automatikus átviteli sebesség alkalmazkodás a csatorna állapothoz. A rosszabb kapcsolatok, melyek általában nagyobb távolságokat képesek átszelni, lassabb sebességet tudnak. További bázisállomások telepítésével csökkenthető a távolság a vezeték nélküli eszköz és a hozzá legközelebb eső access-point között, így növelve az adatátvitel sebességét. Ugyanakkora mennyiségű adat továbbítása kevesebb időt vesz igénybe, így csökkentve a csatornahasználatot.

4. Biztonsági problémák

Alapvető problémák a 802.11-es szabványú hálózatokban:

Fizikai réteghez kapcsolódó veszélyek:

- Bárki hozzáférhet a fizikai közeghez (levegő…)
- Akárki hozzáférhet a hálózathoz nyom nélkül
- A hálózat kiterjedése nem korlátozható (pl. Kijut a Wi-Fi access point jele az épületből.)

4.1. WEP

(Forrás: Joseph Davies – Biztonságos vezeték nélküli hálózatok 2005)

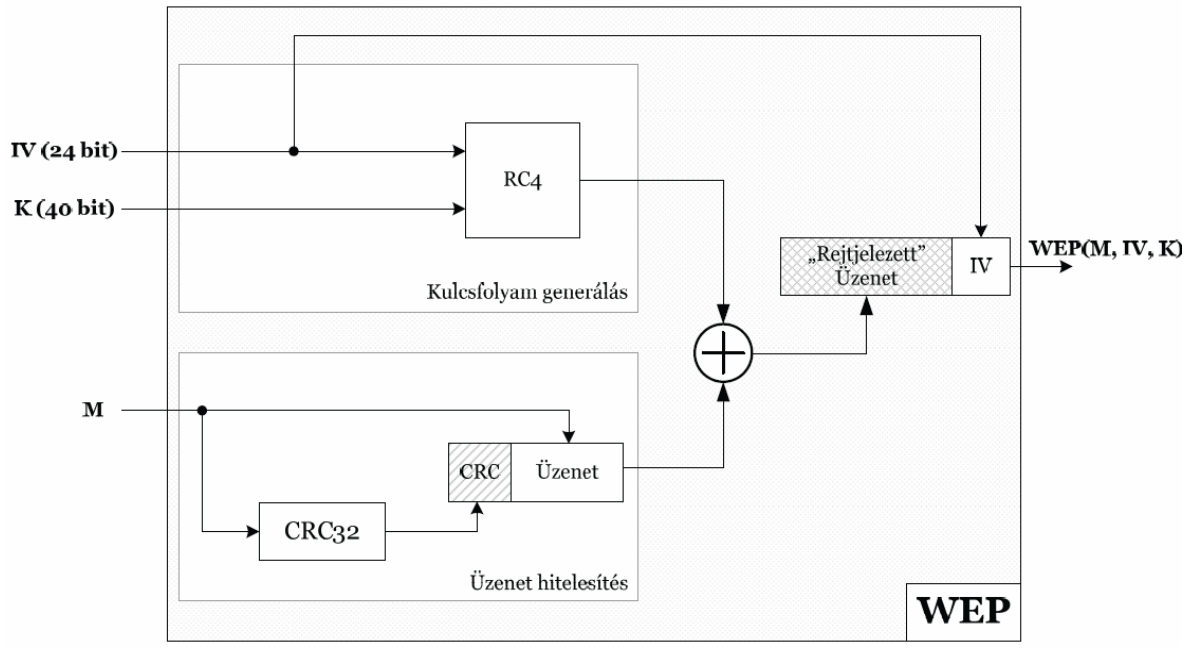
A WEP (Wired Equivalent Privacy = Vezetékessel Egyenértékű (Biztonságú) Hálózat) mára már egy nem korszerű titkosítási algoritmus az IEEE 802.11 vezeték nélküli hálózatok titkosítására. A WEP 1997-ben arra szánták, hogy olyan biztonságos hálózatként működjön, mint egy vezetékes hálózat.

Elemei:

- IV: inicializáló vektor (24 bit)
- K: titkos kulcs (40 vagy 104 bit)
- M: a kódolandó üzenet
- RC4 kulcsfolyam generálásra (OFB módban)
- CRC-32 a hitelesség garantálására (Cyclic Redundancy Check)
- A kulcsfolyamot és a CRC-vel ellátott üzenetet XOR művelettel egyesíti.

A kódolás:

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



WEP Struktúra

Hibák:

Mivel az RC egy stream titkosító, ugyanazt a forgalmi azonosító kulcsot nem szabad kétszer használni. Az IV célja, ami plain text-ként továbbítódik, hogy meggátolja az ismétlődést, de egy 24 bites IV nem elég hosszú, hogy ezt biztosítsa egy forgalmas hálózaton. A mód, ahogy az IV-t használják, az összefüggő-kulcs támadás számára is törhetővé tette a WEP-et. Egy 24 bit-es IV esetén 50% esély van, hogy ugyanaz az IV jelenik meg 5000 csomag után.

2001. augusztusában Scott Fluhrer, Itsik Mantin, és Adi Shamir közétettek egy kripto-analízisét a WEP-nek, amely kihasználja azt, ahogy az RC4 titkosít és ahogy az IV-t használja a WEP. Eredményként egy passzív támadási módot kapunk, ami képes visszafejteni az RC4 kulcsot, miután lehallgattuk a hálózatot. Attól függően, hogy mekkora az adatforgalom, illetve a vizsgálható csomagok száma, a sikeres kulcs visszafejtés akár 1 perc alatt is sikerülhet.
Ha nem elegendő csomagot küldtek, akkor vannak módok arra, hogyan tud egy támadó olyan üzeneteket a hálózatra küldeni, amelyre biztosan választ kapva megtalálhatja a kulcsot. Ezt a támadási módot rövid időn belül implementálták automatizált segédprogramokban.
Ilyen jellegű támadáshoz nem kell más, mint egy PC és egy ingyenesen letölthető szoftver, mint például az aircrack-ng.

Egy 2003-as felmérés két újabb hiányosságát fedezte fel a WEP-nek:

- A WEP használata opcionális volt, ezzel azt eredményezve, hogy az eszközök többségén be sem volt kapcsolva.

- A WEP nem tartalmazott kulcs menedzsment protokollt, helyette egyetlen megosztott kulcsot használt a felhasználók között.

2007-ben Erik Tews, Andrei Pychkine, és Ralf-Philipp Weinmann továbbfejlesztett támadással álltak elő, amely képes volt egy 104 bit-es WEP kulcsot 50%-os valószínűséggel visszafejteni, mindössze 40 000 elfogott csomaggal. 60 000 csomagnál a siker valószínűsége 80%, 85 000-nél pedig már 95%. Aktív támadási technikákat használva (deauthentikáció, ARP újrabeadás) 40 000 csomagot kevesebb mint 1 perc alatt be lehet gyűjteni, maga a számítás pedig egy 2 GHz-es PC-n 2-3 másodpercet vesz igénybe.

Mára a WEP annyira elavult és könnyen feltörhető, hogy a nagyobb cégek biztonsági szabályzatában ki van kötve, a WEP titkosítást használni nem lehet.

NEM BIZTONSÁGOS

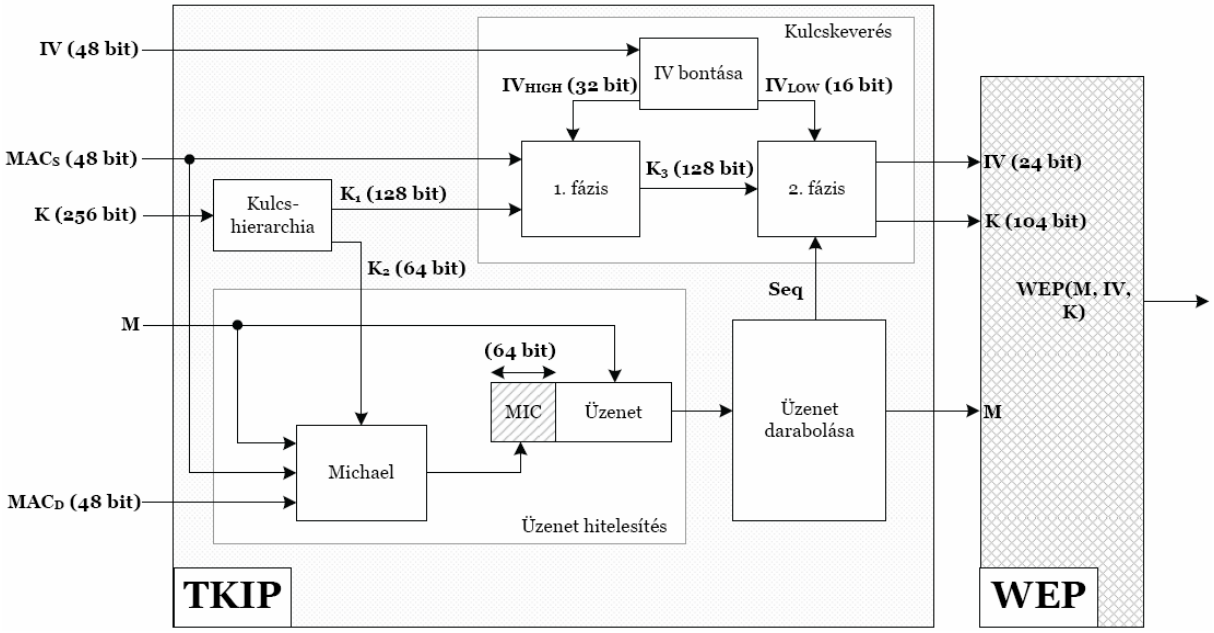
4.2. WPA

(Idézet: http://ethicalhacking.hu/wpa.aspx)

„A vezeték nélküli hálózatokon már régóta ajánlott a WPA (Wireless Protected Access) használata. Ez a titkosítási mód ugyanis kiküszöböli a WEP eddig megismert összes hiányosságát, ezek közül a legfontosabbat, az ismétlődő Initilization Vectort (mely a kulcsgenerálás során felhasznált „random" érték). Az IV-nek kulcsszerepe van a WEP titkosításban, ennek ellenére egy gyenge algoritmus készíti, emiatt akár néhány percen belül is előfordulhat, hogy két csomagot ugyanaz az IV titkosítja. Ezt a problémát úgy oldotta meg az IEEE bizottság, hogy az eredeti 24 bitesről 48 bitesre növelte az IV hosszát, ezzel gyakorlatilag eltüntette az IV ismétlődést, ez az egyik alapja a WPA-titkosításnak.

Azonban a bizottság nem készíthetett teljesen új titkosítást, hiszen biztosítani kellett a visszafelé való kompatibilitást (a régebbi, csak WEP-re hitelesített eszközöknek is támogatniuk kellett az új rejtjelezést). Ezért nyúltak vissza a WPA megalkotói az 1999-ben kiadott 802.11i szabványhoz, és felhasználták az abban meghatározott TKIP (Temporal Key Integrity Protocol) technikát. Ezzel lett teljes a WPA szabvány. A WPA2 ettől abban különbözik, hogy tartalmazza és megköveteli a TKIP mellett az AES (Advanced Encryption System) titkosítást is.

De térjünk vissza az áldozatra, a WPA-ra, amely még nem követeli meg az AES használatát. A visszafelé való kompatibilitás olyan „jól" sikerült, hogy a kutatók végül is megtalálták egy darabját a WEP-örökségnek, amely benne maradt az utódban is: a régebbi kártyákon is működnie kellett a WPA-nak, ezért megmaradt az RC4 kódoló algoritmus és hibadetektálásként az Integrity Check Value, mely WEP esetében nem más, mint a jó öreg CRC32. Ezek együttesen lehetővé teszik az alábbiakban ismertetett ChopChop-támadás alkalmazását WPA-n is.



WPA-TKIP Struktúra

A ChopChop támadás általános működése

A WEP-csomag hibátlanságát CRC32-ellenőrzőösszeg állapítja meg. A hálózati forgalomban ugyan mind az adat, mind a CRC titkosítva utazik, de ha módosítunk a titkosított adatokon, a CRC újraírása révén még a megváltoztatott csomagokat is hitelesként fogadja el az AP. Emiatt a titkosítás megfejtése nélkül, vakon felül lehet irkálni a WEP-csomagokat, és addig lehet kalapálni, amíg a titkosított CRC is helyes lesz.

Ezt a „képességünket” felhasználva lehetőség adódik egy találgatós játékra. Fogunk egy csomagot, kiveszünk belőle egy bájtot. Ez lesz a titok számunkra. Vajon mi volt benne eredetileg? 0-tól 255-ig bármi lehetett. Tegyük fel, hogy amit levágtunk, annak tartalma 42. Újraszámítjuk a csonkolt csomag CRC-jét úgy, mintha tényleg 42-t vágtunk volna le belőle, majd beküldjük őket az AP-nak. Ha a tippünk helyes, a CRC valóban helyes lesz, így a csonka csomagot az AP visszaküldi az éterbe. Ebből tudhatjuk, hogy nyertünk, 42=42! Ha nem, hátravan még 255 próba, és máris megvan az egyik bájt értéke.

Az eljárást megismételjük a csomag többi bájtjára is, így a kulcs ismerete nélkül el tudjuk olvasni a teljes csomagot. De ez még nem minden! Amint megvan egy teljes csomag cleartext változata, ezt össze kell XOR-olni a titkosított változattal, és megkapjuk a WEP kulcsot.

A következő lépés a ChopChop-támadás alkalmazása WPA esetére. Ehhez először lássuk, mit változtattak meg a WPA-ban, hogy nekünk nehezebb dolgunk legyen.

Bevezették az MIC (Message Integrity Check) fogalmát: ez egy 64 bites karaktersorozat, amely kiegészíti a szimpla ICV-t, így nem csak a könnyen megoldható CRC32 áll ellent a támadónak, hanem eme, a Michael-függvénynek nevezett algoritmussal generált összeg is. A másik nagy változás, hogy létrehoztak egy „szekvenciális számolót" és ez vigyáz arra, hogy a csomagok sorrendben érkezzenek a fogadó félhez. A counter működése egyszerű: minden érkező csomag hatására eggyel nagyobb lesz az értéke. Ha aztán később valaki egy rögzített csomagot szeretne visszaküldeni, akkor a nagyobb számlálóérték miatt ez meghiúsul.

A nagyobbik gond azonban az MIC-vel van: ezt nagyon szigorúan veszi a szabvány: ha 2 db MIC hiba fordul elő egy percen belül, akkor leáll a kapcsolat, és egy 60 másodperces szünet után indítja csak el az AP a kapcsolatújrafelvételi-kérelmet a kliens felé – új kulccsal. Ez eléggé behatárolja a támadót.

Ezek után van még valaki, aki elhiszi, hogy sikeres lehet a támadás? Nos, akik igennel válaszolnának, azoknak lett igazuk: igen, még ezek ellenére is véghez lehet vinni. Mi hát a megoldás? A QoS, azaz a Quality of Service WiFi-be integrált megoldása: egy adott csatorna fel van osztva nyolc különböző alcsatornára, így egy eszköz csatornán belül egy másik alcsatornára válthat a kommunikáció folyamán, hogy jobb átviteli minőséget érjen el. „Szerencsére" minden alcsatornához egyedi counter tartozik, valamint a kliensek szinte mindig csak a nullás alcsatornát használják. Ez azt jelenti, hogy szinte mindig találunk egy olyan alcsatornát, ahol alacsonyabb a counter értéke, így a csomagunkat el fogja fogadni az AP!

Sőt, szegény MIC hiába próbál védekezni, kompatibilitási okokból úgy építették fel a WPA-t, hogy először az ICV-ellenőrzés fut le, és ha ez rendben, akkor következik a MIC-ellenőrzés! Tehát a ChopChop által használt, hibás ICV-kre épülő találgatás teljes sebességgel rohanhat egy másik alcsatornán.

Ha az ICV-találgatásunk helyes volt, a feldolgozás végre-valahára eljut a MIC-ig, ami nyilván hibás, mert azt nem tudjuk helyesre pofozni (kapunk egy MIC Failure Reportot). Összegezve: percenkét egy bájtot találhatunk ki, ennyit adott nekünk a szabvány.

Tetszőleges csomagon 8 perc alatt ki tudjuk találgatni a MIC (8 bájt) titkosítatlan értékét, ami később még jól fog jönni. Kellene még egy plaintext, hogy az egészet beletehessük egy megfordított Michael algoritmusba (mivel a függvényt kétirányúnak tervezték) és megkapjuk a titkosításhoz használt MIC kulcsot. Honnan szedjünk plaintextet?

Most jön a csavar. Ha ARP csomagot használunk fel, ami könnyen felismerhető jellegzetes hosszáról (42 bájt), abban már egy csomó adatot eleve ismerünk, hiszen az ARP-ben IP-címek és MAC Addressek utaznak! A MAC Addresseket tudjuk, mert titkosítatlanul repülnek az Ethernet fejlécben (különben nem ismernék fel a csomagot a hálókártyák), általában az IP-címtartományt is ismerjük. Mindössze két bájtot nem ismerünk belőle: a két IP-cím utolsó bájtját!

A két IP-bájtot két ChopChop-pal kitaláljuk (2 perc), és most már kezünkben tartjuk a teljes clear textjét egy WPA-val titkosított csomagnak!

Valóban ez lenne a helyzet? Nem, válaszolhatjuk egyértelműen: a kapott kulcsfolyammal ugyan bekódolhatunk egy csomagot, de a counteren nem változtathatunk, ezért újból a QoS csatornák között kell keresgélnünk, míg meg nem találjuk a megfelelőt, amelyen alacsonyan áll még a counter. A 0-son kommunikál a célkliens, így marad ideális esetben 7 csatornánk a saját gyártmányú csomagok sugárzására. A támadó így már tud kárt okozni, de elolvasni nem tudja az átküldött tartalmat. Ennek ellenére ez így is kellőképpen veszélyes! Az alkalmazható támadások közül az ARP poisoning az első ötlet: úgy állítja át a gépeket a hálózatban, hogy végül minden kommunikáció rajta keresztül menjen végbe.

A támadás működőképességét kutatók bizonyították egy valós hálózaton, sőt megoldást találtak a QoS csatornákat nem támogató AP-k esetére is: ez esetben meg kell akadályozni a kliens-AP kapcsolatot a támadás idejére (így nem nő a counter értéke), pontosan abban a pillanatban, amikor elkaptuk a megfelelő csomagot.

Ha valakinek sikerülne a mindkét irányban érvényes MIC kulcsot megszereznie (ez a támadás ugyanis csak az AP-kliens irány MIC kulcsát fedi fel) és egy valós kulcsfolyamot az egyik QoS csatornára (a counter szempontjából kedvezőre) akkor bármilyen tartalommal bármennyi csomagot küldhet a hálózatnak.

Védekezés

Állítsuk a rekeying intervallt alacsony értékre, pl. 120 másodpercre. Ennyi idő alatt a támadó csak 1, maximum 2 bájtját szerezte meg a MIC-nek, és a kulcsok máris kicserélődnek."
(Idézet vége: http://ethicalhacking.hu/wpa.aspx)

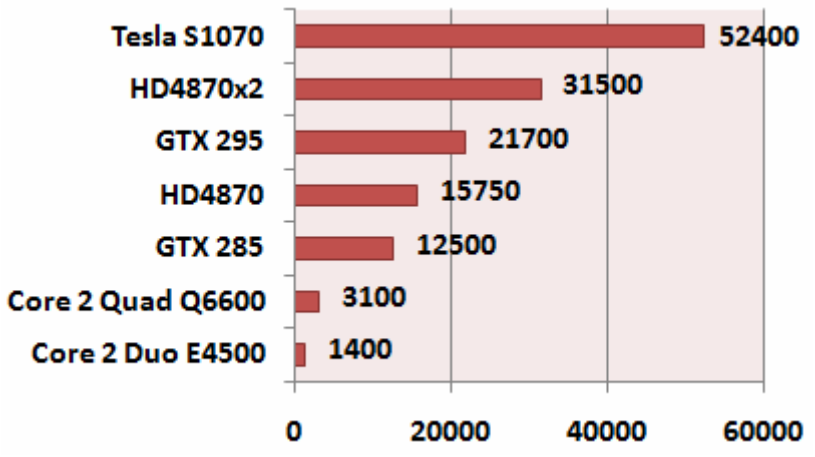
A jelenlegi helyzet

Több ingyenesen letölthető szoftver található a piacon, amelyek együttes használatával fel lehet törni a WPA kódot:

- Kismet: a hálózat elemzésére szolgáló program
- Airforge: deauthentikációs kérés küldése az acces pointnak
- Aireplay: csomag elfogó és küldő program
- Cowpatty: Jelszó feltörő program

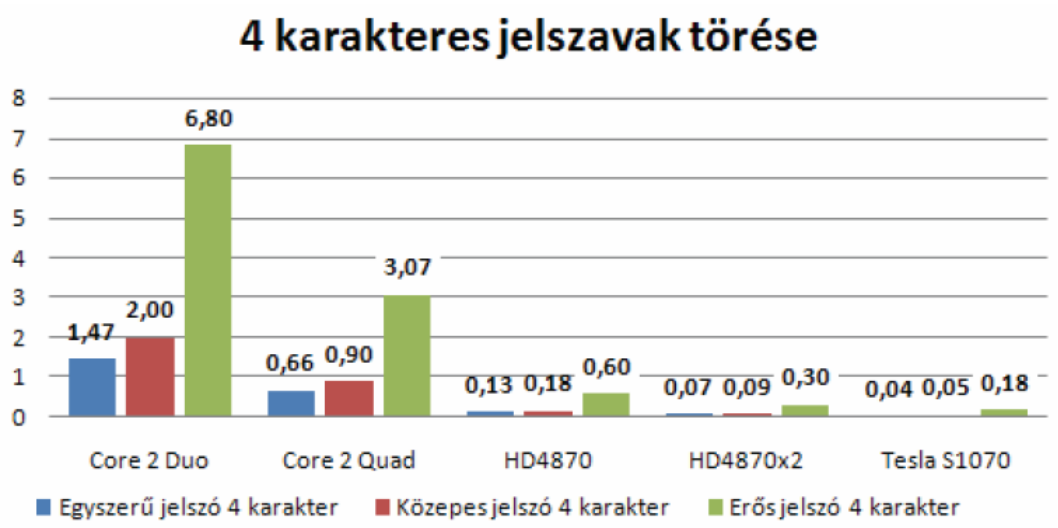
Új technika, hogy a videókártyák párhuzamos számolási képességeit kihasználva sokkal gyorsabban visszafejthetők a WPA kulcsok.
Például egy orosz biztonságtechnikai cég 1.199 €-ért árulja Elcomsoft Wireless Security Auditor névre keresztelt programját, ami kifejezetten nvidia videókártyákhoz lett tervezve és állításuk szerint 100x gyorsabban képes feltörni a WPA/WPA2-PSK kódot, mint a korábbi programok.

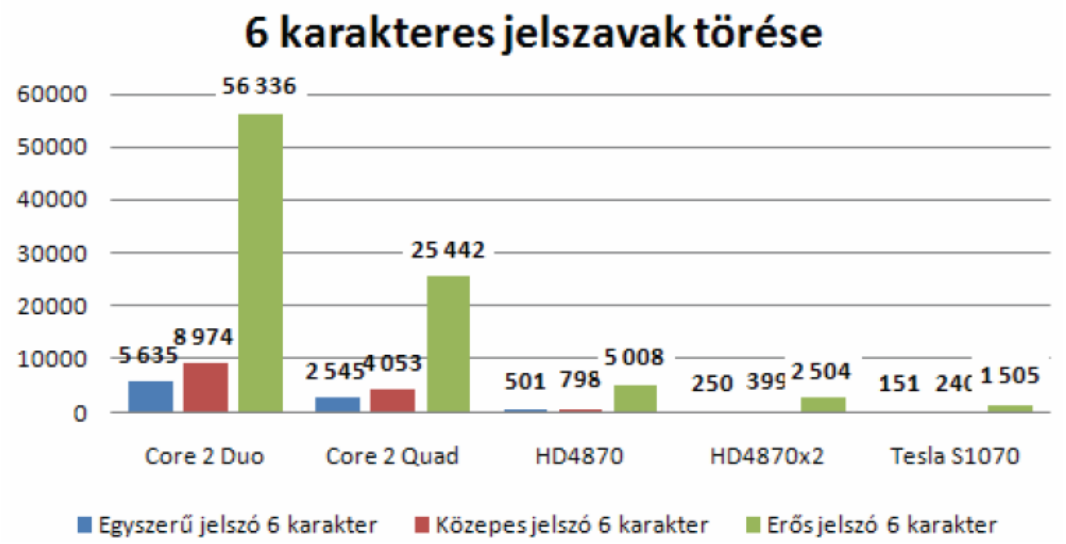
A következő grafikon a program sebességét mutatja:

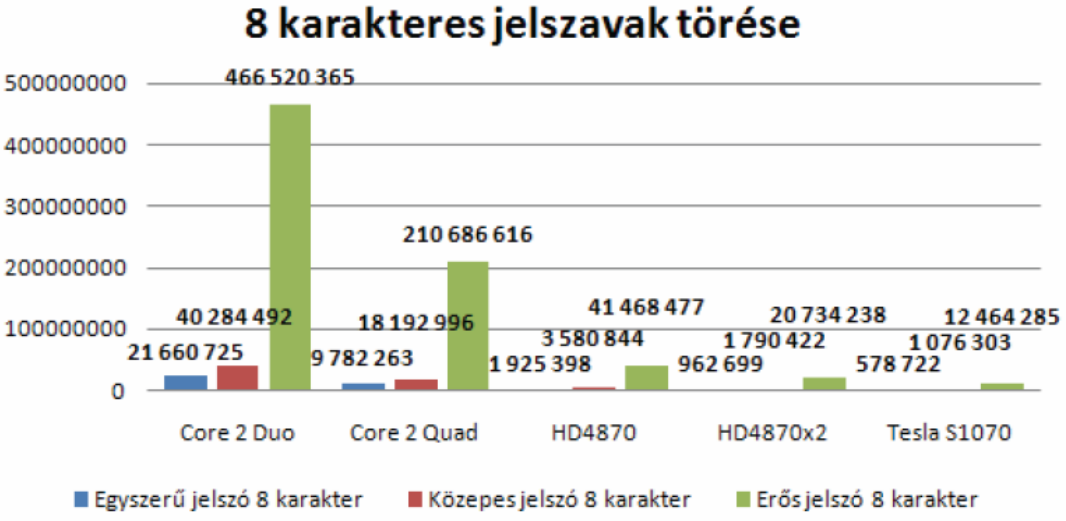


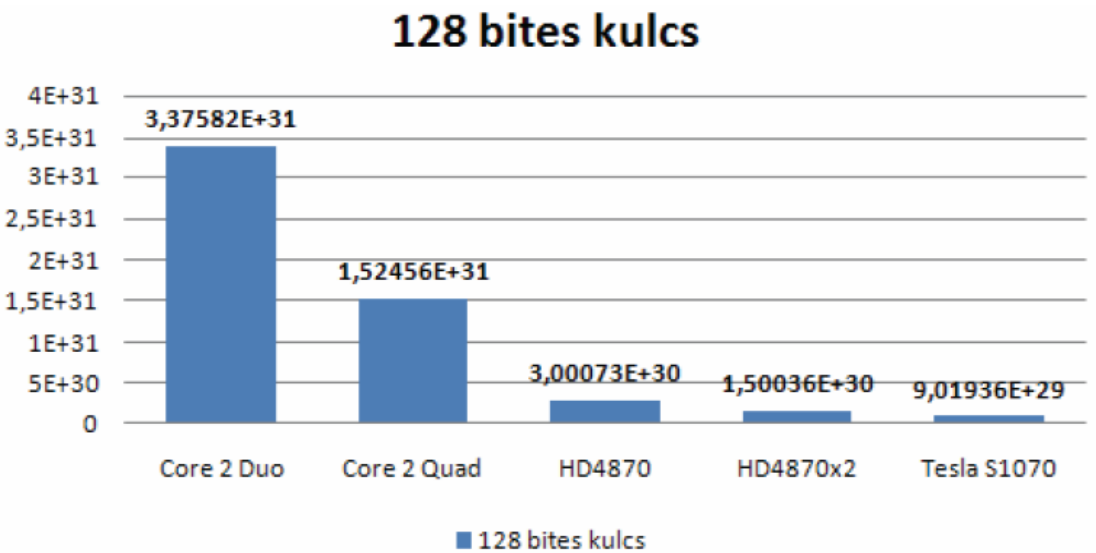
Jelszó / másodperc

Jelen pillanatban a következőképpen alakul a WPA jelszavak feltörésének sebessége (nem a fentebb említett program), attól függően, hogy milyen erős jelszót használunk:









Jelenleg egy jól megválasztott jelszóval konfigurált WPA2-őt használó hálózat valós időn belül „elvileg” nem törhető fel.

4.3. Driver hibák

Jelenleg a piacon számos 802.11-es chipset található, amelyet a gyártók mind másképp implementálnak termékeibe tekintet nélkül a driverek biztonsági réseire.

2006-ban David Maynor és Jon Ellch az akkori Black Hat konferencián bemutatták, hogyan képesek rendszerszinten átvenni a hatalmat egy Apple MacBook felett, kihasználva annak vezeték nélküli kártyájának driverbeli hibáit. Az erről készült bemutató videó itt található: http://www.youtube.com/watch?v=-VY8xYK4z-Q

Ez volt a kezdete annak a folyamatnak, amely során több nagy gyártó chipset-jét érintő driver hibákat kezdtek találni.

Az eddig felfedezett driver hibák közül néhány fontosabb:

CVE-2007-1218 (PARSER)	Off-by-one buffer overflow in the parse_elements function in the 802.11 printer code (print-802_11.c) for tcpdump 3.9.5 and earlier allows remote attackers to cause a denial of service (crash) via a crafted 802.11 frame. NOTE: this was originally referred to as heap-based, but it might be stack-based.
CVE-2007-0933 (DRIVER/WIN)	Will be released today
CVE-2007-0686 (DRIVER/WIN)	The Intel 2200BG 802.11 Wireless Mini-PCI driver 9.0.3.9 (w29n51.sys) allows remote attackers to cause a denial of service (system crash) via crafted disassociation packets, which triggers memory corruption of "internal kernel structures," a different vulnerability than CVE-2006-6651. NOTE: this issue might overlap CVE-2006-3992.
CVE-2007-0457 (PARSER)	Unspecified vulnerability in the IEEE 802.11 dissector in Wireshark (formerly Ethereal) 0.10.14 through 0.99.4 allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2006-6651 (DRIVER/WIN)	Race condition in W29N51.SYS in the Intel 2200BG wireless driver 9.0.3.9 allows remote attackers to cause memory corruption and execute arbitrary code via a series of crafted beacon frames. NOTE: some details are obtained solely from third party information.
CVE-2006-6332 (DRIVER/LIN)	Stack-based buffer overflow in net80211/ieee80211_wireless.c in MadWifi before 0.9.2.1 allows remote attackers to execute arbitrary code via unspecified vectors, related to the encode_ie and giwscan_cb functions.
CVE-2006-6125 (DRIVER/WIN)	Heap-based buffer overflow in the wireless driver (WG311ND5.SYS) 2.3.1.10 for NetGear WG311v1 wireless adapter allows remote attackers to execute arbitrary code via an 802.11 management frame with a long SSID.
CVE-2006-6059 (DRIVER/WIN)	Buffer overflow in MA521nd5.SYS driver 5.148.724.2003 for NetGear MA521 PCMCIA adapter allows remote attackers to execute arbitrary code via (1) beacon or (2) probe 802.11 frame responses with an long supported rates information element. NOTE: this issue was reported as a "memory corruption" error, but the associated exploit code suggests that it is a buffer overflow.
CVE-2006-6055 (DRIVER/WIN)	Stack-based buffer overflow in A5AGU.SYS 1.0.1.41 for the D-Link DWL-G132 wireless adapter allows remote attackers to execute arbitrary code via a 802.11 beacon request with a long Rates information element (IE).
CVE-2006-5972 (DRIVER/WIN)	Stack-based buffer overflow in WG111v2.SYS in NetGear WG111v2 wireless adapter (USB) allows remote attackers to execute arbitrary code via a long 802.11 beacon request.
CVE-2006-5882 (DRIVER/WIN)	Stack-based buffer overflow in the Broadcom BCMWL5.SYS wireless device driver 3.50.21.10, as used in Cisco Linksys WPC300N Wireless-N Notebook Adapter before 4.100.15.5 and other products, allows remote attackers to execute arbitrary code via an 802.11 response frame containing a long SSID field.
CVE-2006-5710 (DRIVER/OSX)	The Airport driver for certain Orinoco based Airport cards in Darwin kernel 8.8.0 in Apple Mac OS X 10.4.8, and possibly other versions, allows remote attackers to execute arbitrary code via an 802.11 probe response frame without any valid information element (IE) fields after the header, which triggers a heap-based buffer overflow.
CVE-2006-3992 (DRIVER/WIN)	Unspecified vulnerability in the Centrino (1) w22n50.sys, (2) w22n51.sys, (3) w29n50.sys, and (4) w29n51.sys Microsoft Windows drivers for Intel 2200BG and 2915ABG PRO/Wireless Network Connection before 10.5 with driver 9.0.4.16 allows remote attackers to execute arbitrary code via certain frames that trigger memory corruption.
CVE-2006-3509 (DRIVER/OSX)	Integer overflow in the API for the AirPort wireless driver on Apple Mac OS X 10.4.7 might allow physically proximate attackers to cause a denial of service (crash) or execute arbitrary code in third-party wireless software that uses the API via crafted frames.
CVE-2006-3508 (DRIVER/OSX)	Heap-based buffer overflow in the AirPort wireless driver on Apple Mac OS X 10.4.7 allows physically proximate attackers to cause a denial of service (crash), gain privileges, and execute arbitrary code via a crafted frame that is not properly handled during scan cache updates.
CVE-2006-3507 (DRIVER/OSX)	Multiple stack-based buffer overflows in the AirPort wireless driver on Apple Mac OS X 10.3.9 and 10.4.7 allow physically proximate attackers to execute arbitrary code by injecting crafted frames into a wireless network.
CVE-2006-1385 (PARSER)	Stack-based buffer overflow in the parseTaggedData function in WavePacket.mm in KisMAC R54 through R73p allows remote attackers to execute arbitrary code via multiple SSIDs in a Cisco vendor tag in a 802.11 management frame.
CVE-2006-0226 (DRIVER/BSD)	Integer overflow in IEEE 802.11 network subsystem (ieee80211_ioctl.c) in FreeBSD before 6.0-STABLE, while scanning for wireless networks, allows remote attackers to execute arbitrary code by broadcasting crafted (1) beacon or (2) probe response frames.

Megoldás

Mindig legyenek naprakészek a vezeték nélküli eszközeink driverei, hogy egy már felfedezett hibát a támadók, ne tudjanak még időben kihasználni!

(Forrás: http://www.blackhat.com/presentations/bh-europe-07/Butti/Presentation/bh-eu-07-Butti.pdf)

4.4. Wardriving és Piggybacking

Wardriving az tevékenység, amikor egy mozgó járműből, vagy gyalog egy Wi-Fi-t támogatót eszköz segítségével Wi-Fi hálózatokat keresünk.

A wardriving szó az 1983-as WarGames című filmből származó wardialing kifejezésből ered, amiben is számítógép-rendszerekhez akartak csatlakozni egy program segítségével, ami sorban tárcsázott telefonszámokat, hogy olyat találjanak, amelyhez számítógépet csatlakoztattak.

Piggybacking az a tevékenység, amikor egy vezeték nélküli eszközzel csatlakozunk valaki Wi-Fi hálózatához és használjuk annak Internet kapcsolatát, a tulajdonos beleegyezése vagy tudta nélkül. Jogilag vitatott kérdés, hogy törvénysértő-e ez a tevékenység. Magyarországon már született ezzel kapcsolatban jogerős ítélet:

Részlet az [origo] 2007. 11. 29-ei cikkéből:

(http://www.origo.hu/techbazis/internet/20071129-a-szabad-wifihasznalat-lopasnak-minosul.html)

Idén nyáron adtunk hírt arról, hogy egy nyitott wifi-hálózatot internetezésre használó fiatalembert kapott el a rendőrség. Azóta megszületett a szabálysértési határozat és az elsőfokú bírósági ítélet is: lopással elkövetett tulajdon elleni szabálysértésért figyelmeztetésben részesítették a fiatal felhasználót. Az okozott kár kilenc forint volt.

Lopásnak minősül a wardriving

Fellebbezés után a Szegedi Városi Bíróság tárgyalás nélkül hozott ítéletében helybenhagyta a szabálysértési hatóság határozatát, ami végül jogerőre emelkedett. Így született meg a - vélhetően első - hazai wardriving ítélet, amely szerint a védtelen hálózatra való csatlakozás lopásnak számít. Az első ítéletet nyilván befolyásolta az is, hogy adatforgalmi korlátos kapcsolatot használt a hálózatát nyitva hagyó ügyfél, így a kár mérhetővé vált. A károsult saját becslése szerint 3,79 megabájtnyi adat csorgott le az internetről azalatt az idő alatt, amíg ő maga ugyan nem netezett, de a fiatalember a ház előtt tartózkodott. A házban lakó, adatforgalmi korlátos internet-előfizetési csomaggal rendelkező ügyfél kára ez alapján 8,63 Ft volt, amit a határozatban kilenc forintra kerekítettek fel.

A fiatal "elkövetőnek" lehetősége lett volna meghallgatást kérnie a bíróságtól, ezzel azonban nem élt, így emelkedett jogerőre az ítélet. Hazánkban ugyan nincs precedensítélkezés (azaz azonos ügyben születhetne teljesen más ítélet is), mégis sokan úgy tekintettek erre az ügyre, hogy egyértelműsíti a hatóságok bizonytalankodó álláspontját. Még a történet elején a rendőrségi jegyzőkönyv rögzítette, hogy a helyszínen lefoglalt számítógép asztalán olyan ikont találtak, amelyik a kilenc forintos kárt szenvedett lakó vezetéknevével volt jelölve, s mellyel két kattintással rá lehetett csatlakozni a hálózatkoz. A határozat szerint már csak a vezetéknév is utalt arra, hogy az általa használt hálózat "idegen hely", s aki idegen dolgot mástól elvesz, az lopást követ el.

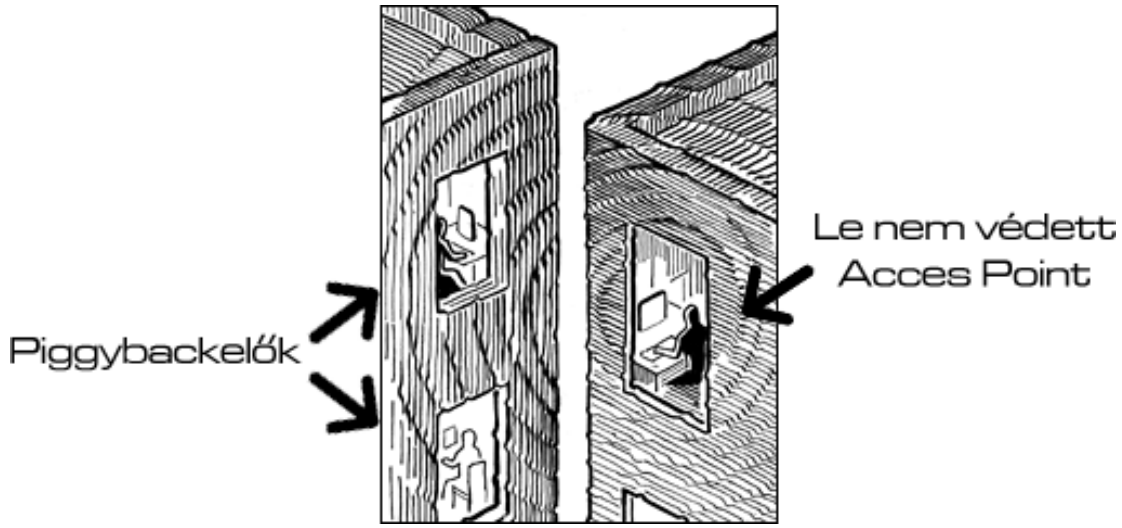
Adatforgalom bemondásra

A szabálysértési határozat ellen a fiatalember azért nyújtott be kifogást, mert szerinte az adott időszakban bárki használhatta az internetet - lévén az teljesen védtelenül volt felkínálva az utcai járókelőknek. A bíróság előtt ugyan nem érvelt ezzel, de lapunk érdeklődésére kifogásolta azt is, hogy a hatóság az okozott kárt bemondásra elhitte, semmi nem bizonyítja, hogy azt az adatforgalmat egyedül ő generálta. Nyilván nem a kilenc forintnyi károsszeg a jelentős, hanem, hogy az, hogy a lopás tényét bemondásra elhitte a hatóság.
Másrészről érthető az is, hogy az internet előfizetője aggódott a ház előtt laptoppal bóklászó ismeretlen miatt, hiszen egy adatforgalmi korlátos hozzáférésnél nem jó ómen, ha többen

használják az internetet - ki tudja mire. Ekkor viszont felmerült kérdés: ha nem akarta, hogy idegenek használják internetkapcsolatát, miért nem védte le a hálózatát?
Sokak szerint méltányos, sokak szerint nem

Türk István, a hazai vezetéknélküli közösség egyesületének, a Huwico korábbi elnöke érdeklődésünkre elmondta: szerinte egy ilyen ítéletnek az elrettentő szerepe megkérdőjelezhető, ám ebben az esetben méltányosnak tartja. Türk elsősorban annak a felelősségét boncolgatta, aki nyitva hagyja az eredetileg otthoni használatra szánt hálózatát, hiszen köztudott, hogy a rádiójelek nem állnak meg a szobák falainál. Ugyanakkor korábban is jelezte: az, hogy létezik egy nyitvahagyott hálózat, még nem jelenti azt, hogy az korlátlan internet-hozzáférést biztosít a járókelőknek.

Olvasóink a korábbi cikkünk után kifejtett véleményeikben is inkább arra az álláspontra helyezkedtek, hogy aki nem teszi biztonságossá az otthoni internetkapcsolatát, az magára vessen, ha illetéktelen felhasználást tapasztal. Az internetes érdekvédő szervezetek ugyanakkor arra figyelmeztettek: sok esetben álnaívság azt hinni, hogy minden nyitott hálózat közkincs, amit bárki szabadon használhat. A közvélekedésre némiképp rácáfolta hozta meg ítéletét a bíróság: a védtelen hálózatokra belépni, és ott internetezni ugyanis lopás, még akkor is a hálózat tulajdonosa - hanyagságból vagy hozzá nem értésből -szabad hozzáférést biztosít.
[*origo*]



Egy életből vett példa a Piggybackelésre

Megelőzés

A törvényeknek nincs meg a fizikai képessége, hogy meggátolják a hasonló cselekedeteket.
A vezeték nélküli hálózatok tulajainak van képessége megakadályozni, hogy „kívülről" hozzáférjenek a hálózathoz-→ megfelelő biztonsági lépéseket kell tenni!
Ezeket nem minden tulajdonos teszi meg, valamint egyes lépések hatásosabbak, mint a többi.

Lépések egy biztonságos hálózat eléréséhez:

- Bár a WEP a profik szerint szinte, olyan mintha nem is lenne ott, mégis az olyan hobbyfelhasználók számára védelmet nyújtanak, akik meg akarják védeni saját hálózatukat a velük azonos tudási szinten lévő betolakodóktól (pl. piggyback-előktől).
- WPA és megfelelő jelszó használatával biztosítható, hogy hálózatunkhoz valós időn belül ne tudjanak hozzáférni.
- MAC cím authentikációval és DHCP-vel szerver beállításokkal létre lehet hozni egy engedélyezett MAC cím listát. Ezzel a biztonsági megoldással az AP csak olyan számítógépeknek fog IP-t adni, amiknek a MAC címe a listában megtalálható. Persze így az adminisztrátornak kell begyűjtenie a MAC címeket minden egyes lehetséges kliens készülékéről, valamint későbbiekben is managelni kell ezt a listát. Ez a módszer nem véd az adatlopástól, mivel nincs titkosítás a folyamatban.
- IP security-t (IPsec-et) használhatunk a hálózati csomópontok közötti adatátvitel titkosítására, megszüntetve ezzel az adatok kódolatlan formában történő továbbítását. Az IPsec beállítása problémába ütközhet, attól függően, hogy milyen márkájú AP-t használunk. Bizonyos esetekben firmware frissítésre lehet szükség, hogy az AP támogassa az IPsec-et. Ez a védelem jelenleg valós időben nem törhető fel, így biztonságot nyújt az adatainknak.
- VPN beállítások, mint például tunnel-mode IPsec vagy OpenVPN nehezen beállíthatóak, de gyakran ezek nyújtják a legrugalmasabb, bővíthető biztonsági megoldást.
- Vezeték nélküli IDS-eket (intrusion detection systems) használhatunk Rogue AP-ok detektálására, amelyek biztonsági réseknek teszik ki a hálózatot. Ezeket a rendszereket általában nagyobb vállalatok szokták alkalmazni, ahol sok user van.

5. Esettanulmány

A mindennapos problémák bemutatása Wi-Fi John, egy nagyvállalati dolgozó szemszögéből…

Bevezetés

Egy dzsungel van odakint, különösen most, hogy milliók dolgoznak távolról, újabb és újabb kihívások elé állítva az IT infrastruktúrájukat és gyakran tudtukon kívül minden nap veszélyeztetik a cégük biztonságát. Mostani kutatások azt mutatják, hogy 3 éven belül, megközelítőleg 1 milliárd mobil dolgozó (távmunkás) lesz világszerte, így a biztonságos, gyors, és megbízható távoli kapcsolat problémái csak nőni fognak.

A távmunkás szemszögéből nézve, gyors információ létfontosságú a munkájukat nézve. Függetlenül attól, hogy otthon vannak, vagy a Föld másik oldalán, a sebesség és a megbízhatóság a kulcs, hogy sikeresen tudják végezni a munkájukat.
Az IT részleg szemszögéből nézve, minden dolgozó igényét ki kell elégíteni, míg folyamatosan szem előtt kell tartania a biztonsági előírásokat, ami egyre nagyobb kihívás, most, hogy a dolgozók többsége kilépett a vállalat falain kívülre.
A legfőbb kérdések:

- Össze lehet egyeztetni ennek a két egymással szemben álló csoportnak a munkáját?
- A távoli hozzáférés akárhol is legyünk, lehet egyszerre gyors és biztonságos?

A Valóság

Felületesen vizsgálva a következő forgatókönyv ártalmatlannak tűnhet…, egy átlagos dolgozó átlagos napja. Azonban rejtett problémákkal találkozunk szinte mindenhol, melyek később kivizsgálásra kerülnek.

Wi-Fi John Nagy Napja

Reggel 6 óra van, a gyerekek készülődnek az iskolába, és Wi-Fi John - egy mítikus távmunkás, aki a Sales részleg alelnöke egy nagyobb vállalatnál – a dolgozószobájába tart, hogy megnézze az email-jeit. Megmozdítja az egerét, hogy felébressze a céges laptopját, elindítja az email kliens-t, majd megvárja míg a levelek letöltődnek. Nem érti, hogy miért tart olyan sokáig letölteni az emaileket, és nem tetszik neki a tény, hogy ez időt emészt fel, amit a feleségével és a gyerekivel is tudna tölteni, mielőtt mindenki indul otthonról a dolgára. Míg vár, elindítja a böngészőt, megnézi részvényeinek árfolyamát, meglátogat néhány oldalt, hogy értesüljön a legfrissebb hírekről és megnézi milyen idő várható a városban, ahova a nap későbbi részében utazni fog. Mikor az emailek végre letöltődtek, válaszol néhány fontosabb levélre és megjelöl még párat, melyekkel később fog foglalkozni. Összepakolja a laptopját, és sietve készülődik, hogy el tudjon indulni.

Wi-Fi John első állomása a reptér. A járata szokás szerint késik, így a reptéri Wi-Fi-t használja, hogy megnézze az ügyfél adatait, akivel találkozni fog. Megpróbálja elérni a cége ERP rendszerét (Enterprise Resource Planning), de az annyira lassú, hogy biztos benne, a rendszerrel van a baj. Feladja az ERP rendszert és a CRM rendszerrel (Customer Relationship Management) próbálkozik, de ugyanezt a problémát tapasztalja. Felhívja a cég help desk-jét, vár míg felveszi valaki, majd azt mondják neki, hogy a rendszerekkel minden rendben van. Ez nem az, amit Ő lát, de mit tehet? Frusztrált, és a szükséges adatok nélkül száll fel a gépre.

Pár órával később Wi-Fi John megérkezik az aznapi első megbeszélésére. Bekapcsolja a laptopját egy konferenciateremben és csatlakozik az Internethez az ügyfél hálózatán keresztül. Csatlakozik a céges intranethez és letölti a prezentációt, amin az emberei a repülőút alatt dolgoztak. A prezentációja részeként, idegesen indítja el a streamelt videót. Ideges, mert korábban többször is annyira lassú volt a streamelés, hogy tovább kellett lépnie a videót, és tudja, hogy ez nem hagy jó benyomást az ügyfelekben. Szerencsére a prezentáció egész jól megy ma, néhány kisebb várakozással megszakítva a videót, de az ügyfél egy sor kérdést tesz fel neki, amiket nem tud megválaszolni, mert korábban a reptéren nem tudott hozzáférni a céges alkalmazásokhoz.

Van egy szabad órája, amit el kell ütnie a következő megbeszélésig, így megáll a sarki kávézóban egy gyors cappuchinora. Amíg élvezi az italát, elindítja a laptopját és a kávézó hot spot-ját használva, újra megpróbálja elérni a céges programokat. Bár a rendszer még mindig lassú, sikerül letölteni a következő ügyfélhez szükségeses adatokat.

Még hagy egy feljegyzést, hogy küldjön majd egy emailt az IT részleg vezetőjének, mikor visszaér, hogy kiderítsék mi a baj a rendszerrel. Ahogy készül összepakolni, egy hírt lát, miszerint egy híres bank elnökének az személyes adatait ellopták adathalász módszer segítségével. Egy nyugtalan érzés fogja el, ráébred, hogy ha ez egy bank elnökével megtörténhet, akkor akárkivel megtörténhet, beleértve magát is. Kíváncsi, hogy a személyes adatai az irodán kívül is biztonságban vannak-e.

A következő találkozón egy új problémával szembesül. Az ügyfél biztonsági előírásai miatt nem tudja használni a laptopját, így az ügyfél konferencia termében lévő PC-t kell használnia. Bár nem teljesen nyugodt, hogy az ügyfél gépével csatlakozik a cége rendszeréhez, nincs más választása, mert másképp csalódást okozna az ügyfélnek. A prezentáció jól megy és meg tudja válaszolni az ügyfél kérdéseit, felhasználva a kávézóban letöltött adatokat.

A találkozó befejeztével a reptér felé veszi az irányt, ahol a járata ismét késik. Elindítja a laptopját letölti az emailjeit, válaszol a fontosakra, és visszatér a korában megjelöltekre. Megnyitja az egyik emailt és eszébe jut a történet a bank elnökről, amint észreveszi, hogy a levél nem attól jött mint ami a feladóban volt írva és reméli, hogy nem tett semmi csúnya dolgot a laptopjával vagy a személyes adataival.

Késő este ér haza, segít lefektetni a gyerekeket, a dolgozószobájába megy, elküld még pár emailt, megnéz pár kedvenc oldalt és megy aludni, tudván, hogy holnap minden kezdődik előről.

És ami a színfalak mögött játszódott

Nézzük meg, mi is történt a színfalak mögött, míg a távmunkásunk végigment a tipikus napján.

Wi-Fi John 5 különböző access point-on keresztül fért hozzá a céges programokhoz, melyek közül egy sem az Ő cége birtokában volt. A megfelelő biztonsági beállítások hiányában Wi-Fi John többször is veszélynek tehette ki a céges rendszert, a laptopját, vagy a személyes adatait. Számos esetben ideges volt a rossz válaszidők és az aggódás miatt, hogy valami rosszul sül el, amikor az ügyfélnek éppen online prezentációt tart.

Hogy a dolgok még rosszabbak legyenek, Wi-Fi John az IT részleget okolja az idegeskedésének okaiért – nem tudnák Őt jobban segíteni? Végülis, Ő a Sales alelnök, Ő az aki az arcát adja a cégnek minden nap, Ő rajta múlik minden.

Nézzük meg Wi-Fi John napjának állomásait, hogy megértsük mi történt és milyen biztonsági veszélyeknek volt kitéve minden állomásnál.

Otthon

Wi-Fi John a napját az emailek letöltésével és néhány weboldal megtekintésével kezdte. A lassúság, amit az emailek letöltése közben tapasztalt, több okból is származhat. Hirtelen sok távmunkás akarta egyidőben letölteni az emailjeit az email szerverről és ez túlterhelte a szervert.

A cége WAN-ját akkor tervezték, amikor még sokkal kevesebb távmunkás volt. Most, feltehetőleg az összes dolgozó 1/3-a dolgozik távolról, valamilyen időszakban, és egyre komplexebb módon terhelik a vállalati WAN-t. Ha a távmunkások csak emailt töltenének le, akkor sebesség még elfogadható lenne. De manapság a dolgozók komplex vállalati alkalmazásokat nyitnak meg, prezentációs videókat streamelnek, és egyre többen használnak VoIP-t. Ezek az alkalmazások képesek nagy adatforgalmat generálni. Ezek a dolgok mind hajlamosak belassítani a vállalati WAN-t.

Továbbá Wi-Fi John-nak valószínűleg ugyanolyan hozzáférési jogosultsága van, mint bármely másik alkalmazottnak a cégnél, tekintet nélkül az Ő személyének a fontosságára a cégben, és a jó adatkapcsolatra való igényre, amikor ügyfelekkel tárgyal. Kevés vállalat képes személyreszabott erőforrásokat biztosítani, a távmunkásai számára. Wi-Fi John cége sem képes erre, pedig a megfelelő beállítással több erőforráshoz juthatna és kevesebbet idegeskedne.

A reptéren

Míg a reptéren Wi-Fi John céges alkalmazásokat próbált elérni a gépe indulása előtt, annak ellenér, hogy Ő a magára a rendszerre gyanakodott, a probléma valójában az Internet csatlakozásával volt. Ha cége irodájában lett volna, akkor nem tapasztalta volna semmilyen problémát az alkalmazásokkal.

Egyik ok, ami hat a webes alkalmazások sebességére az az, hogy ezek webes szolgáltatásokat használnak. A XML-re épülő webes szolgáltatások közismerten nagy adatátvitel igényűek. Amikor egy web szolgáltatás alapú alkalmazás lép egy régi kliens-szerver alapú alkalmazás helyébe, akkor gyakran az új alkalmazás sávszél igénye lényegesen több, 10-100x-osa is lehet a korábbinak, ennek oka az XML. Adjuk hozzá ezt a sávszél igény növekedést, a távmunkások számának növekedéséhez és nem meglepő, hogy Wi-Fi John nem tudta megszerezni a számár fontos adatokat a gép indulása előtt.

Wi-Fi John lehet, hogy nem is volt tudatában annak a sok biztonsági kockázatnak, aminek ki volt téve, míg az Internetet használta a céges laptopjáról egy titkosítatlan reptéri Wi-Fi kapcsolaton keresztül. A veszélyeken felül, amit a látszólag ártalmatlan oldalak látogatása és ezzel a kártékony programok települése jelent, lehetséges, hogy olyan emberek kószáltak a reptéren, amelyek levédetlen laptopokat kerestek, hogy feltörjék azokat. Egy profi hacker feltörhette volna a laptopot, adatokat lophatott volna el, és el is tűnt volna a helyszínről, még mielőtt Wi-Fi John észrevehette volna, hogy egyáltalán veszélynek van kitéve.

Az első ügyfélnél

Az első ügyfélnél Wi-Fi Johnnak hozzá kellett férnie a céges szerverhez és alkalmazásokat futtatni az ügyfél Internet kapcsolatán keresztül. Mivel ez egy kisebb cég, elég jó esély van arra, hogy itt a biztonsági előírások nem olyan szigorúak, mint Wi-Fi John cégénél. Wi-Fi John biztonsági kockázatoknak tette ki a laptopját, és az ügyfél access pointján keresztül a cég szerverét, és a céges alkalmazásokat. Még lehet, hogy az ügyfél tűzfalával is bajlódnia kellett, ami újabb kihívást jelentett számára, miközben a prezentációjához akart anyagot letölteni.

A sebesség nagy gondot jelentett számára, mivel nem engedhette meg magának az ügyfél megvárakoztatását, és ha a kapcsolat lassú lett volna, akkor kockáztatja, hogy a videó nézhetetlen lesz. Szerencsére jelen esetben a dolgok jól mentek, de korábban már volt ezzel gondja és lehet, hogy legközelebb is lesz.

A kávézóban

Az összes hely közül, ahol ma Wi-Fi John dolgozott, a kávézóban volt a legnagyobb veszélynek kitéve. Míg a repülőtér és az ügyfél kapcsolata biztosított valamilyen szintű védelmet, addig a kávézóban és szinte az összes többi hotspotnál a biztonsági kicsi, elenyésző. Mint a repülőtéren, Wi-Fi John kártékony programoknak, behatolásnak, adathalászatnak volt kitéve és még sok olyan veszélynek, amiért neki vagy a hozzá hasonlóaknak egyszerűen nincs idejük aggódni. A kávézóban Wi-Fi John szerencsésnek érezte magát, mert sikerült hozzáférnie az alkalmazáshoz, amire szüksége volt a következő tárgyalásához. Nem értette, miért működik ezúttal (lehet, hogy kevesebb távmunkás használta az alkalmazáokat, vagy a wi-fi hotspot-nak volt sok szabad sávszélessége), de egyébként sincs szüksége a folytonos aggódásra, minden alkalommal, mikor el akarja érni a vállalati alkalmazásait.

A második ügyfélnél

A második találkozóján Wi-Fi John rá volt kényszerítve, hogy a cége rendszerét az ügyfél gépén keresztül érje el az ügyfél internetét használva. Akármilyen védelmet is állított be az IT részleg Wi-Fi John laptopján, az innentől kezdve kiesett a játékból, és csak reménykedhetett abban, hogy a céges oldalt is valamilyen beállítások védik, a teljesen ismeretlen, védtelen eszközöktől, amik hozzá csatlakoznak.

Újból a reptéren

Habár Wi-Fi John számára ez a rész ugyanazt a biztonsági kockázatot és sebesség gondokat jelentette, mint korábban mégis ezúttal Wi-Fi John mégis elbukott, mert megnyitott egy olyan levelet, amit úgy hitt, hogy egy ismerőse küldött neki.. Ha az üzenet vírust tartalmazott, akkor tudtán kívül kompromittálhatta a laptopját, a céges rendszerek biztonságát, és még a saját személyes adatait is. A megfelelő védekezési eszközök nélkül Wi-Fi John „elfoglalt napja”, hamar válhat Wi-Fi John „rossz napjává”, vagy még rosszabra Wi-Fi John „Cégének a rossz napja”

Újra Otthon

Habár biztonságban érezhette magát otthon a zsúfolt nap után, Wi-Fi John és a cége megpróbáltatásainak még nincs vége. Amíg „szolgálaton kívül” volt és weboldalakat nézegetett felüdülésképp, megnézhetett olyan oldalakat is, amelyek elvileg biztonságosak, de cyber bűnözők már otthagyták rajtuk a „védjegyüket”. Még a nagy oldalak sem immúnisak az ilyen jellegű támadásokkal szemben, és sem Wi-Fi John, sem pedig az alkalmazottai nincsenek tisztában teljesen ennek veszélyeivel. Egy teljesen biztonságos átjáró nélkül, ami scannel minden átmenő adatot, a legkevésbé sem annak látszó oldalak is tudnak kárt okozni a gépünkben. Nem is említve azt, a kérdést: Vajon Wi-Fi John otthoni access point-ja milyen biztonsági beállításokat tartalmaz. Megvédi-e Őt és cégét a külső támadókkal szemben?

6. Összegzés

Mint ahogy a szakdolgozat bemutatta, a Wi-Fi technológia még relatíve új, és emiatt a kommunikáció minden szintjén kihívásokkal küszködik:

- A Wi-Fi (b/g) a 2.4 GHz-es tartományban működik, aminek használata a legtöbb országban nincs engedélyhez kötve, ezáltal az ugyanebben a tartományban működő más eszközökkel (Bluetooth, Mikrohullámú sütők, vezeték nélküli telefonok, videó megfigyelő rendszerek, stb.) kapcsolatba kerülve interferencia léphet fel, aminek következtében vagy a hálózat teljesítménye csökken, vagy teljesen ellehetetleníti a kommunikációt.

- Az energia fogyasztása magas a többi vezeték nélküli szabványhoz viszonyítva, problémát okozva ezzel az akkumulátorok élettartamára, valamint a hőtermelésre nézve.

- A Wi-Fi hatótávolsága véges. Egy tipikus otthoni Wi-Fi router hatótávolsága beltéren 45 méter, kültéren 90 méter. Természetesen a legújabb 802.11n-es szabvány nagyon ígéretesnek tűnik, a maga több mint kétszeres hatótávolságával és többszörös átviteli sebességével, de ennek elterjedése még kezdeti stádiumban van.

- Az idő előrehaladtával jelennek meg újabb és újabb szabványok. A különböző szabványok (802.11 a/b/g/n) együttes alkalmazása lassíthatja a teljes hálózat teljesítményét, ha nincsenek jól beállítva.

- A leginkább elterjedt vezeték nélküli titkosítási szabvány a WEP feltörhető, még akkor is, ha jól van bekonfigurálva.

- A WPA titkosítási szabvány jelenleg már csak akkor nyújt megfelelő védelmet, ha megfelelő bonyolultságú titkosítási kulcsot használunk. Ebben az esetben a kulcs visszafejtése valós időn belül nem megvalósítható.

- A Wi-Fi eszközeink driverei, tartalmazhatnak hibákat, amit a hozzáértő támadók kihasználhatnak, és rendszer szintű hozzáféréshez juthatnak számítógépeinken.

- A levédetlen Access Point-ok hatalmas biztonsági kockázatot jelentenek. Ezek megfelelő védelme elengedhetetlen.

A Wi-Fi használata megkönnyíti, kényelmessé teszi a mindennapjainkat, azonban tudnunk kell, hogy milyen technológiai és biztonsági problémákkal kell szembenéznünk. Ismernünk kell azokat a módszereket, amikkel ezeket meg tudjuk szüntetni, illetve kockázati tényezőjüket a lehető legkisebbre csökkenti.

7. Irodalomjegyzék

Jim Geier - Vezeték nélküli hálózatok 2005

Stewart Miller - Wi-Fi Security 2003

Joseph Davies – Biztonságos vezeték nélküli hálózatok 2005

http://en.wikipedia.org/wiki/802.11 2009.11.15.

http://en.wikipedia.org/wiki/Electromagnetic_interference_at_2.4_GHz 2009.11.15.

http://ethicalhacking.hu/wpa.aspx 2009.11.15.

http://www.origo.hu/techbazis/internet/20071129-a-szabad-wifihasznalat-lopasnak-minosul.html 2009.11.15.

www.google.com