

A WIFI HÁLÓZATOK VESZÉLYEI

Absztrakt

Az elmúlt néhány évben gomba módra elszaporodtak a wifi hálózatok és Access Pointok ezrei jelentek meg. Nagyszámú elterjedésük legfőbb oka a rugalmasságukban rejlik, segítségükkel, kis szakértelemmel is könnyedén ki lehet alakítani hálózatokat. Mindezt úgy lehet megtenni, hogy nem kell kábelek kötegeinek a boncolgatásától tartanunk. Ám, ahogy az élet minden területén lenni szokott, itt is két oldala van az éremnek: a szakszerűtlen telepítés, a hozzá nem értés kézzelfogható veszélyeknek teszi ki az adott hálózatot. E biztonsági kockázatoknak a létéről sokan nem tudnak, a nyugati példával ellentétben, a köztudatban ezek széles körben nem terjedtek el. Jelen cikkben a wifi hálózatok rövid bemutatása után ezekre a lehetséges kockázatokra kívánjuk felhívni a figyelmet egy-egy ilyen - természetesen teszhálózat elleni - támadás részletes bemutatásával.

Thousands of wifi networks appeared during the last years. The reason for the big number is the flexibility of these networks. Without being an expert and dealing with big amount of wire, you can easily build up practicable networks. But this simplicity could be the death of your network. Several security breaches could threaten your lan. Many times this threat is hidden for the owner. In this paper we would like to show some of these security holes via tests and measures on our testing-lan.

Kulcsszavak: Wifi, 802.11, WEP, WPA, hálózati biztonság, wardriving

BEVEZETÉS

Napjainkra a vezeték nélküli hálózatok egyre nagyobb teret nyernek, gomba módra szaporodnak az access pointok³ (továbbiakban AP). Ezen hálózatoknak hatalmas előnye a mobilitás, de ez az előny sokszor nincs összhangban a velük együtt járó veszélyekkel, biztonsági kockázatokkal, melyeket rádiós, szabadtérben terjedő mivoltuk képez.

Mivel rengeteg írás jelent meg a 802.11 szabványról, a Wifi⁴ hálózatok paramétereiről, működésükről, ezekre csak érintőlegesen szeretnénk kitérni és inkább a konkrét vizsgálatokra fókuszálunk.

A wifi hálózatok elterjedésével együtt járt egy újfajta „sport”, „hobby” elterjedése is, melynek lényege, hogy vezeték nélküli eszközökkel, esetleg GPS⁵-szel kiegészítve, feltérképezik egy adott területen elérhető wifi hálózatokat. Ez a wardriving (gépjárművel), illetve warchalking (gyalog). <http://www.wardrive.net>

¹ hadnagy

² mk. alezredes, ZMNE tanszékvezető egyetemi docens

³ Hozzáférési pont

⁴ Wireless Fidelity, az IEEE által kifejlesztett vezeték nélküli mikrohullámú kommunikációt megvalósító szabvány népszerűsítő neve.

⁵ Global Positioning System

Fontosnak tartjuk megjegyezni, hogy ilyenkor semmilyen illetéktelen behatolási kísérlet nem történik az adott hálózatokra, ahogyan mi sem próbálkoztunk semmi ilyennel, mindazonáltal az elterjedtebb hálózatteltörési módszereket egy saját tesztüzemű hálózaton kipróbáltuk, és ezek tapasztalatait e munkában meg is osztjuk az olvasóval.

Budapest egy nagyobb területét térképeztük fel 2007 áprilisában, az elérhető vezeték nélküli hálózatok szempontjából. Ez a terület a következő volt:



*1. ábra Budapest - részlet
(Forrás: googleearth.com)*

- Budapest: a 47,51,47,89/19,043140 (Margit sziget bejárata a Margit híd felől), valamint a 47,491401/19,120696 (Zách utca-Salgótarjáni utca sarka) koordináták által kifeszített, 5,82km x 2,63km-es téglalap alakú terület, gépkocsival mozogva. Meg kell jegyezni, hogy a hatalmas terület csekély részének bejárása miatt a felderített hálózatok száma csak töredéke a teljes területen fellelhető hálózatok számának, de statisztikai alapnak megfelelőnek tekinthető.

WIFI HÁLÓZATOK

Az első wifi hálózatok megjelenése hivatalosan 1997 júliusára tehető, ekkor jelent meg a 802.11-es IEEE szabvány. Ezek után több szabvány is jelent meg, például a 802.11c, 802.11d, 802.11e, melyek nem témája dolgozatomnak, a továbbiakban csak a széles körben elterjedt, ismertebb típusokkal foglalkozunk.

A 802.11 megjelenését követte 1999 októberében a 802.11a, illetve 802.11b, majd 2003 júniusában megjelent a 802.11g és végül 2007-ben a 802.11n szabvány, mely jelenleg is kialakítás alatt áll.

Ezeknek a hálózatoknak a működése a 2,4Ghz és 5Ghz-es tartomány közé esik, több csatornára felbontva. A földrajzi helytől függően eltérések jelentkeznek a csatornakiosztások között, nem minden csatorna létezik az összes országban. Ilyen jellemző területek a következők:

1. Amerikai/Kanada,
2. Európa – Közel Kelet - Afrika
3. Japán
4. A föld többi része

A következő táblázatban tekintsük át ezen a szabványoknak a sajátosságait. Minden csatornához egy kisebb frekvencia tartomány tartozik, a könnyebb átláthatóság érdekében mindenhol a közép frekvenciákat tüntettük fel. Továbbá fontos megjegyezni, hogy a távolságok névlegesek, ennél jóval nagyobb, akár több kilométeres távolságok is elérhetőek megfelelő antennák beszerzésével. Egyes ilyen távolság orientált versenyeken a 100 km-es távolságok sem ritkák.

Pl.: <http://www.wifi-shootout.com>

1. Táblázat Wifi szabványok (Forrás: www.wikipedia.com)

Szabvány neve / megjelenés dátuma	Elérhető elméleti átviteli sebességek (Mbs)	Moduláció ⁶	Csatorna kiosztás	A csatorna „közép” frekvenciája (MHz)	Amerika	EMEA ⁷	Japán	A világ többi része	Névleges hatótávolság beltérben (m)	Névleges hatótávolság kültérben (m)
802.11b 1999 október	5,5, 11 továbbá kompatibilis a 802.11 2 és 1 Mbps adatátviteli sebességével is	kétfajta modulációs eljárás támogatott: Alapértelmezett a CCK ⁸ , de ez felcserélhető a PBCC ⁹ -vel	1	2412	X	X	X	X	35	100
			2	2417	X	X	X	X		
			3	2422	X	X	X	X		
			4	2427	X	X	X	X		
			5	2432	X	X	X	X		
			6	2437	X	X	X	X		
			7	2442	X	X	X	X		
802.11g 1999 október	6, 9, 12, 18, 24, 36, 48, 54 továbbá kompatibilis a 802.11b 5,5 és 11 Mbps sebességével, és a 802.11-el 1 és 2 Mbps sebességgel	OFDM ¹⁰ Emellett képes együttműködni a 802.11b CCK modulációval	8	2447	X	X	X	X	25	75
			9	2452	X	X	X	X		
			10	2457	X	X	X	X		
			11	2462	X	X	X	X		
			12	2467	—	X	X	X		
			13	2472	—	X	X	X		
			14	2484	—	—	X	—		
802.11a 2003 június	6, 9, 12, 18, 24, 36, 48, 54	OFDM	34	5170	—	X	—	—	25	75
			36	5180	X	—	X	—		
			38	5190	—	X	—	—		
			40	5200	X	—	X	—		
			42	5210	—	X	—	—		
			44	5220	X	—	X	—		
			46	5230	—	X	—	—		
			48	5240	X	—	X	—		
			52	5260	X	—	—	X		
			56	5280	X	—	—	X		
			60	5300	X	—	—	X		
			64	5320	X	—	—	X		
			149	5745	—	—	—	—		
			153	5765	—	—	—	—		
			157	5785	—	—	—	—		
			161	5805	—	—	—	—		

⁶ Olyan eljárás, amely lehetővé teszi, hogy biteket vigyünk át elektromágneses hullámok segítségével. Főbb típusai az amplitúdó illetve a fázis vagy frekvencia moduláció. A WLAN fázismodulációs eljárásokat használ.

⁷ Európa, Közel-Kelet, Afrika

⁸ Complementary Code Keying

⁹ Packet Binary Convolutional Code

¹⁰ Orthogonal Frequency-Division Multiplexing

A Wifi hálózatokat egy másik szempont alapján két nagy csoportba lehet osztani:

- nyílt
- titkosított hálózatok

A fenti táblázatban fellelhető összes szabvány támogatja a nyílt, illetve titkosított csatornák használatát, viszont nem minden hálózati eszköz kompatibilis ezekkel. Általánosságban elmondhatjuk, hogy minél régebbi az eszköz annál szerényebb szolgáltatást, így titkosítási eljárást támogat.

Nyílt Wifi hálózatok

Ezen hálózatoknak legfontosabb és egyben leghátrányosabb tulajdonsága, hogy a rajta továbbított adatok teljesen nyíltan, úgynevezett „plain text” formában kerülnek továbbításra, egy esetleges támadó szöveges formában képes olvasni az átvitt adatot, mint például jelszavakat.

Az alábbi ábrán egy webes bejelentkezése folyamata látható egy titkosítatlan hálózaton a „teszt felhasználó”, „test jelszó” felhasználónév/jelszó párossal.

5d 49 64 3d 63 6f	.,.....f ormId=co
73 41 75 74 68 26	mmmands.P lusAuth&
74 70 25 33 41 25	backurl= http%3A%
51 69 6c 2e 68 75	2F%2F[redacted]email.hu
55 73 25 32 46 61	%2Flevel ezes%2Fa
5d 64 25 33 44 63	uth.fm%3 Fcmd%3Dc
36 70 61 67 65 25	heckuser %26page%
73 26 63 6d 64 3d	3Dlevele zes&cmd=
55 6d 6f 74 65 66	plusauth &remotef
3d 74 65 73 7a 74	orm=1&us er=teszt
5c 6f 40 66 72 65	+felhasz nalo@[redacted]
73 65 72 77 69 74	[redacted]mail.hu &userwit
3d 74 65 73 7a 74	houtdoma in=teszt
5c 6f 26 70 61 73	+felhasz nalo&pas
5c 73 7a	s=teszt+ jelsz

2. ábra Sniffing
(Készítették: a szerzők)

Manapság általában három esetben találkozhatunk ilyen „elavult ” hálózat típussal:

1. Az eszközök régiek, nem támogatják az újabb titkosító eljárásokat.
2. Újabb eszköz esetén gyári, úgynevezett „default” beállításokkal kerül telepítésre a hálózat, mely nagyfokú veszélynek van így kitéve.
3. Egyes szolgáltatók ilyen formában nyújtanak internet szolgáltatást, melynél az elsődleges szempont a könnyű konfigurálhatóság a kliens részéről. Ilyenkor úgynevezett „captive portálok”, magyarra fordítva elkapó, begyűjtő portálok kerülnek alkalmazásra a hálózat hozzáférés szabályozásának céljából, mely a kliens számára védelmet nem nyújt.

Captive portálok működése röviden:

Miután a kliens sikeresen asszociál az AP-tal minden http request egy központi captive portálra kerül átirányításra, ahol a kliensnek felhasználónév/jelszó párossal kell magát azonosítania az AP illetve a szolgáltató tűzfala felé. Sikeres azonosítás után számára alagút nyílik a MAC address / IP címe alapján a külvilág irányába és innentől már a böngésző http request-jei a megfelelő irányba lesznek továbbítva.

Titkosított Wifi hálózatok

Ebben a fejezetben a wifi hálózatok titkosításának lehetőségeit mutatjuk be a teljesség igénye nélkül. Mivel cikkünk figyelem felkeltő célú és a WPA¹¹ TKIP¹² és WPA AES¹³ hálózatok megfelelő beállítás esetén megbízható biztonságot nyújtanak, azok rendszerspecifikációjával ebben a cikkben részletesen nem foglalkozunk.

WEP¹⁴

A legelső, széles körben elterjedt titkosítási eljárás wifi hálózatok számára. Bár a 802.11 szabvány tervezésekor már megjelent az igény a biztonságra, ezt a WEP alkalmazásával nem érték el, a biztonság messze alulmaradt az elvárásoknak. Ennek fő oka a hibás protokolltervezés volt. Egy WEP alapú hálózat feltörése ma 2-7 óra között kivitelezhető, ahogy azt saját teszt üzemű hálózaton ki is próbáltuk.

Hogy jobban megértsük a WEP gyengeségét meg kell vizsgálni annak működését. Vezeték nélküli hálózatoknál általában három biztonsági kérdés merül fel:

1. a hálózat lehallgatása
2. a hálózat szolgáltatásainak illetéktelen használata
3. a hálózat bénítása

A WEP az első két problémára próbált megoldást kínálni. Az első problémát a forgalom titkosításával, a másodikat az eszközök hitelesítésével szeretne volna megoldani.

¹¹ Wi-Fi Protected Access

¹² Temporal Key Integrity Protocol

¹³ Advanced Encryption Standard

¹⁴ Wired Equivalent Privacy

Hitelesítés

Minden eszköznek a forgalmazás megkezdése előtt hitelesítenie kell magát az AP felé, mely egy négy lépcsőből álló üzenetváltásból áll. Ezt a folyamatot mutatja a 2. táblázat.

2. Táblázat:

A mobil állomás jelzi egy „authenticate request” küldéssel a hitelesítési szándékát az AP felé.

Az AP generál egy véletlenszerű számot és azt elküldi a mobil állomásnak. Ez az „authenticate challenge”

A mobil állomás rejtjelzi ezt a számot a beállított WEP kulcsával és visszaküldi az eredményt az AP-nak „authenticate respond” formában.

Ha az AP ezt dekódolni tudja, akkor a két eszközön beállított kulcs egyezik, tehát az állomás csatlakozhat a hálózathoz.

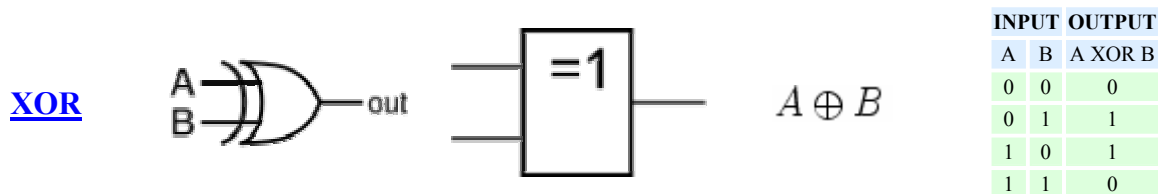
Az AP a dekódolás eredményét közli a mobil állomással „authenticate success” vagy „authenticate failure” formában.

Rejtjelzés

A hitelesítés megtörténte után az adatforgalom titkosított formában történik, melynek kulcsa ugyanaz, mint amit a hitelesítéshez használnak. A titkosításhoz használt algoritmusnak az RC4¹⁵ folyamkódolót választották.

RC4 alkalmazása a WEP-ben

Az RC4 folyamkódoló a többi folyamkódolóhoz hasonlóan a következőképpen működik: egy pár byte méretű titkos kulcs, jelen esetben a WEP kulcs segítségével egy jóval hosszabb álvéletlen byte sorozatot állítanak elő, majd ezzel és a XOR¹⁶ matematikai művelet segítségével rejtjelzik az adatfolyamot.



3. ábra a XOR művelet

(Forrás: http://en.wikipedia.org/wiki/Logic_Gate)

¹⁵ ARCFOUR folyamatitkosító

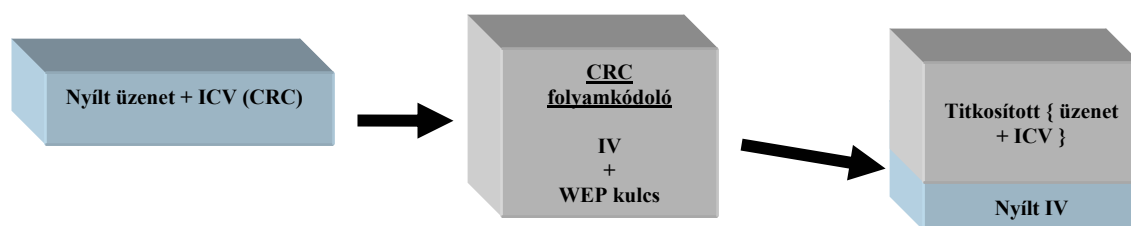
¹⁶ Logikai kizáró VAGY művelet

A WEP-es alkalmazáskor ez egy-két apró módosítással kiegészül. Annak elkerülése érdekében, hogy minden üzenetváltáskor ugyanazt a titkos kulcsot használjuk, a WEP kulcs mindig kiegészítésre kerül egy „IV¹⁷”-vel, mely üzenetenként változik. Így elkerülhető, hogy egyszerűbb statisztikai módszerekkel feltörhető legyen a titkosítás.

A másik apró módosítás, hogy a nyílt üzenethez mindig hozzáfűzésre kerül egy ICV, ami nem más, mint a nyílt üzenetre számolt CRC¹⁸/ellenőrző összeg, mely a nyílt üzenettel együtt kerül titkosításra. Ennek a CRC-nek egyik célja lenne, hogy kizárják a szándékos módosításokat. Mint később azt látjuk ez a funkció sem „bomba biztos”.

Tehát a titkos WEP kulcs, valamint az üzenetenként egyedi IV segítségével előállítjuk a hosszú álvéletlen sorozatot, majd ezzel és a XOR művelet alkalmazásával titkosítjuk az üzenetet, végül a túloldali dekódolás érdekében az üzenethez hozzáfűzzük az IV-t nyíltan.

A könnyebb megértést segíti a következő ábra.



4. ábra A WEP titkosítás folyamata
(Készítették: a szerzők)

A dekódolás ugyanígy, fordított sorrendben történik.

A WEP hiányosságai, sebezhetőségei:

Itt kell néhány szót ejteni a WEP kulcsokról, azok hosszáról, megbízhatóságukról. Általában a WEP kulcsok 104 bit hosszúak, ehhez adódik hozzá a 24 bit hosszú IV. Így jön ki a köztudatban szereplő 128 bites titkosítás, ami félrevezető, hiszen ebből 24 máris nyílt, mint, ahogy azt az előzőekben láttuk. A 104 bit hosszú kulcsok helyett eleinte 40 bit hosszút használtak, amit 64-bites titkosításként is ismerünk (40bit + 24 bit IV). Ezek szerencsére már kihalóban vannak. Létezik még a 256, valamint 152bit-es WEP is de ezek elterjedtsége alacsonyabb.

Eszközök konfigurációjakor a kulcsot két formában lehet megadni nekik, az eszközöktől függően. Ez lehet hexa, illetve karakteres formában ábrázolva: a 40 bites WEP kulcsot 5 karakter megadásával, míg a 104 bitet 13 karakter megadásával érhetjük el. (Egy karakter 8 biten ábrázolható: 8bit x 5 = 40 bit; 8bit x 13 = 104bit)

¹⁷ Initialization Vector (Induló vektor)

¹⁸ Cyclic redundancy check.

3. Táblázat: A WEP kulcsok kialakításának logikája (Készítették: a szerzők)

WEP	IV hossz	Kulcs hossza bitekben	Kulcs hossza hexa formában	Kulcs hossza ASCII jel formában	Kulcs ASCII karakter formában	Az ASCII karakter alapú kulcs hexa megfelelője
64 bit	24	40	10 karakter	5 karakter	„abcde”	„6162636465”
128 bit	24	104	26 karakter	13 karakter	„abcdefghijklm”	„6162636465666768696a6b6c6d”
152 bit	24	128	32 karakter	16 karakter	„abcdefghijklnop”	„6162636465666768696a6b6c6d6e6f 70”
256 bit	24	232	58 karakter	29 karakter	„abcdefghijklnopqrstuvwxy z123”	„6162636465666768696a6b6c6d6e6f 707172737475767778797a313233”

Eszközők konfigurációjakor érdemes kulcsgenerátorokat alkalmazni, sok ilyet találhatunk az interneten, pl.: <http://www.andrewscompanies.com/tools/wep.asp>

A továbbiakban a WEP biztonsági kérdéseire is ki kell térni, melyek egy részét kipróbáltuk a teszthálózaton.

A WEP hibái

1. A hitelesítés egyirányú, mindig csak a mobil állomás hitelesíti magát, így sohasem lehetünk biztosak, hogy a saját bázisállomásunkhoz (AP) csatlakoztunk és nem egy támadó által felállított, ugyanolyan nevű AP-n keresztül jutnak el az adataink a célba.
2. A hitelesítés csak a hálózathoz való csatlakozás pillanatában egyszer történik meg. Ezután már bárki küldhet üzenetet az egyszer már hitelesített kliens nevében, annak MAC address-ét használva. Elsőre azt gondolhatnánk, hogy ez nem lehet baj, hiszen a támadó nem ismeri a WEP kulcsot, így ennek semmi értelme. De ha a támadó egy elkapott, titkosított üzenetet küld vissza, akkor arra az AP titkosított formában újra és újra válaszolni fog. Ez a kiinduló pontja az úgynevezett visszajátszásos, angol nevén „replay” alapú támadásoknak, ahogy, azt később bemutatjuk.
3. A hitelesítés és a rejtjelzés ugyanazzal a kulccsal történik, így az egyik megszerzésekor a másik birtokába is jutunk.
4. Ha a támadó elkapja a hitelesítés előzőekben bemutatott 4 teljes ütemét, akkor az „A” kihívásból és a rá kapott, $T = A \text{ xor } K$ válaszból képes kiszámítani a „K”-t ($A \text{ xor } T = K$), aminek birtokában bármilyen kihívásra - „authenticate challenge” - képes válaszolni a kliens nevében.
5. Az integritás védelem sem hibamentes: a CRC lineáris voltából adódóan a támadó az üzenet bármely bitjét képes úgy módosítani, hogy közben nem is ismeri az üzenet tartalmát. Általánosságba elmondható, hogy CRC védelem lenne hivatott kivédeni az üzenet visszajátszásos támadásokat, ami a WEP-ből teljesen hiányzik.
6. Titkosítás. A legnagyobb biztonsági rést pont maga a rejtjelzés jelenti: a problémát a lehetséges IV-k beláthatóan véges száma adja. Mint azt már említettük az IV 24 bit hosszúságú, ami kb. 17 millió lehetséges IV-t jelent. Tapasztalatok szerint ideális körülmények között egy támadás közben 60-70 IV-t lehet másodpercenként gyűjteni. $70 \text{ IV} \times 60 \times 60 = 252.000 \text{ IV} / \text{óra}$. $16.777.216 / 252.000 = 66,5 \text{ óra}$. Ez azt jelenti, hogy 67 óra hallgatóság után már ismétlődnek az IV-k. Tovább rontja a helyzetet, hogy általában az IV-k nem véletlenszerű helyről, hanem mindig nulláról indulnak, így több eszköz esetén hamarabb előfordulnak ugyanazok az IV-k. Az ebben a pontban felsoroltakat kihasználva kriptográfusok egy csapata egy bonyolult statisztikai, valószínűségi alapokon nyugvó támadó algoritmust készített,

amivel a valóságban már 200.000 - 500.000 összegyűjtött IV alapján sikeres támadást lehet indítani a WEP kulcs ellen.

WPA

A WEP hibái nem sokkal megjelenése után már napvilágot láttak és az IEEE új biztonsági megoldások után nézett. Teljesen új alapokon és algoritmusokon nyugvó rendszert dolgozott ki a wifi hálózatok védelmére. Mivel ez egy jóval összetettebb és bonyolultabb eljárás, annak hosszadalmas részletezését most ebben a munkámban mellőzöm és csak ismeretterjesztő jelleggel összefoglaljuk ennek az új szabványnak a fontosabb újításait.

Egyik legfontosabb módosítás az adatátvitel során alkalmazott új titkosító algoritmus. A régi RC4 folyamkódolót leváltotta az AES algoritmus. Itt kell megjegyezni, hogy ez a váltás a régi típusú készülékeken software és firmware frissítéssel nem megoldható, mindenképpen új hardware-t igényel, így egy további irányzatot is kialakítottak: annak érdekében, hogy a régi eszközökből egy software frissítés után a WEP-nél erősebb védelmű hálózatot lehessen kialakítani. Ez a hálózat továbbra is az RC4 folyamkódolót használja több módosítással. Ezt az irányvonalat nevezték el WPA TKIP-nek, míg az AES algoritmust használó WPA lett a WPA2, vagy másik nevén WPA AES.

További fontos újítás, hogy itt már külön kulcs van a hitelesítésre és az adatfolyam titkosításra, sőt még az integritás védelemre is.

A hitelesítés teljesen új alapokra került, a forgalmazás során dinamikusan változik a titkosításhoz használt kulcs. Az ilyen hálózatok IV-k gyűjtésével már nem törhetőek, egy hitelesítési folyamatot kell elkapni, majd ez ellen szótár alapú támadást intézni. Ez megfelelően erős kulcsválasztás esetén akár több évtizedig is eltarthat.

WIFI HÁLÓZATOK FELMÉRÉSE, AZOK TÁMADÁSA

A wifi hálózatok biztonsági kockázatairól általában

Sokat hallunk veszélyekről, melyek hálózatunkat, számítógépeinket fenyegethetik. Ebben a fejezetben át szeretném tekinteni azokat a kockázatokat, amik kifejezetten a vezeték nélküli, azok közül is a nyílt vagy gyenge titkosítást használó hálózatokra jellemzőek. A továbbiakban a WEP alapú hálózatok könnyű feltörhetősége miatt ezt a két fajta hálózatot egynek tekintjük és egy részben tárgyaljuk.

Mindenképpen első helyen kell megemlíteni a számítógépeink védelmét: bárki, aki hatótávolságon belül helyezkedik el, kontrolálatlan formában hozzáférhet a számítógéphez, megfelelő tűzfal és vírusvédelem hiányában az azon futó operációs rendszer biztonsági réseit kihasználva hozzájuthat az összes rajta tárolt adatahoz, a rajta begépelte jelszóhoz, stb.

Ennek sikertelensége esetén még mindig a támadó előtt nyitva áll a teljes hálózati forgalom lehallgatásának lehetősége, aminek során felhasználónevekhez, jelszavakhoz, személyes adatokhoz, felhasználói szokásokhoz juthat. Bár egy banki azonosítónak - a bank és a felhasználó közötti titkosított kapcsolat miatt - így közvetlenül nem jut a birtokába, de gondoljunk bele, hogy mi történhet, ha ezt a banki jelszavát más szerveren is használja, aminek irányába az adatkapcsolat nem biztos, hogy titkosított, mint például az email postafiókjá...

Manapság egyre nagyobb problémát jelentenek a zombi hálózatok, az azok által indított spam áradat, illetve DoS¹⁹ támadások. A védtelen hálózatok könnyen áldozatául eshetnek ilyen tömeges támadást kiszolgáló törekvéseknek.

Ennél is nagyobb problémát jelenthet, ha valamilyen célzott betörést a mi hálózatunkról indítanak, amit még vissza is követnek. Képzeljük el, ahogy magyarázkodni próbálunk egy internetes betörés gyanúsítottjaként.

Wifi hálózat „elrablása”

A következőkben egy érdekes technikát is megismertetünk az olvasóval, amivel egy wifi hálózat feletti teljes irányítás átvehető. Célunk vele, hogy felhívjuk a figyelmet erre az interneten terjedő veszélyre, a szakszerűtlenül, vagy egyáltalán be sem konfigurált eszközök hátrányaira.

A támadás alapfeltétele, hogy az AP gyári, azaz default admin jelszóval üzemeljen. Ez sajnos nagyon sok esetben így van: a vásárló megveszi, kibontja, összedugja és használja mindenféle beállítás nélkül.

További feltétele, hogy java engedélyezett böngészővel egy előre elkészített kártékony oldalra tévedjen a felhasználó.

A téma megértéséhez szükséges az AP-ok konfigurálásának egy minimális szintű ismerete. A legtöbb AP konfigurálása WEB-es felületen keresztül történik, valamilyen böngésző használatával. Fontos megjegyezni, hogy ez, alapállapotban csak a hálózat „belső” oldala felől lehetséges, a külvilág, például az Internet irányából nem.

A technika lényege, hogy miután az internetet böngésző felhasználó egy olyan oldalra jut, ami egy kártékony kódot tartalmaz, a felhasználó böngészője a háttérben letölti és elindítja azt. A letöltött kód ekkor már a felhasználó gépén fut a hálózat belső oldalán, ahol a számítógép IP címéből kiindulva megpróbálja feltérképezni a hálózatot, az AP IP címét. Ezzel nem lehet sok problémája, mivel gyári beállítások esetén ez 2-3 érték lehet, általában 192.168.2.1. Ha ezzel végez, akkor megpróbál egy web böngészőt utánozva kapcsolatba lépni az AP-tal, megpróbálja annak kezdőlapját lehívni, pl.: <http://192.168.2.1>. Ezután kiértékeli a weblap felépítését, annak grafikai elemeit. Ezt összeveti a saját eszköztárával és megkeresi pontos típusra lebontva, hogy melyik eszköznek van ugyanolyan kezdőlapja, mint amivel találkozott. Ezt elképzelni így lehet: „a web lap jobb felső sarkában van egy 131 kbyte hosszú jpg file, melynek neve smc.jpg. Ez melyik AP-ra illik?”. Ezután az ehhez az AP-hoz tartozó gyári jelszóval illetve utasításokkal megpróbálja tetszés szerint átkonfigurálni a routert. Például új DNS²⁰ servert állít be, melynek eredményeképpen elérheti, hogy egyes WEB lapok behívásakor az eredeti oldalak helyett a támadó saját web serverén előre elkészített web oldal töltődjön be. Például egy banki kezdőlap...

¹⁹ Denial of Service attack / szolgáltatás leállítási támadás

²⁰ Domain Name Server

Eszközök

A felméréshez, valamint a hálózat biztonságának teszteléséhez kizárólag kereskedelmi forgalomban kapható eszközöket használtunk. Ezek egy-kettő kivételével könnyen beszerezhetőek.

A felméréshez használt valamennyi program az internetről letölthető.

Mivel a dolog jórészt a wifi kártyán áll vagy bukik, arra részletesen is kitérünk:

Általában a wifi kártyák nem alkalmasak támadó jellegű tevékenységekre. A speciális funkciók, mint például az eszköz promiscuous üzemmódban (ami a hálózati forgalom figyeléséhez, illetve csomaginjektáláshoz szükséges) történő üzemeltetése csak bizonyos chipset-ű (Atheros, Prism) kártyákkal valósítható meg. További jellemzőjük, hogy áraik a kibővített képességek miatt jóval a „hétköznapi” kártyák felett van.

A felmérések során használt hardware:

- HP nx 8220 laptop beépített bluetooth képességekkel.
- HTC 3300 PDA beépített GPS vevővel, bluetooth képességekkel.
- „SuperRange Cardbus 300mW 802.11 a/b/g” PCMCIA wireless kártya
- 5 dB nyereségű botantenna MMCX aljzattal
- 18,6 dB nyereségű Yagi antenna, RPTNC aljzattal. Horizontális nyílásszöge 18° , vertikális nyílásszöge 18°. A nagytávolságú felderítés mellett iránymérésre, az AP-ok földrajzi helyzetének meghatározására, valamint a gyengébb teljesítményű mobil eszközök forgalmának távolról történő megfigyelésére is hasznos.
- N – RPTNC antenna kábel a Yagi antennához.
- N – MMCX pigtail (a wifi kártya és az antenna kábel közé)

Felhasznált, kipróbált software-ek:

Software-ek Linux

- Back Track 2 Linux LIVE CD
- Red Hat Fedora 6 Linux

Software-ek linux alatt:

- Airmon, Kismet,
Airodump, Aireplay,
Aircrack, Wireshark,
Airsnoort, Ettercape

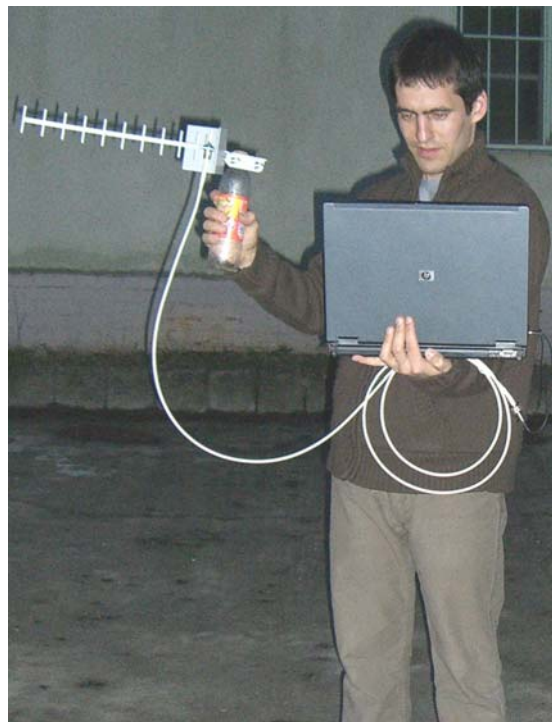
Software-ek Windows alatt:

- Wirelessmon²¹
- Netstumbler - ingyenes program

²¹ <http://www.passmark.com/products/wirelessmonitor.htm>



5. ábra Kellékek
(Készítették: a szerzők)



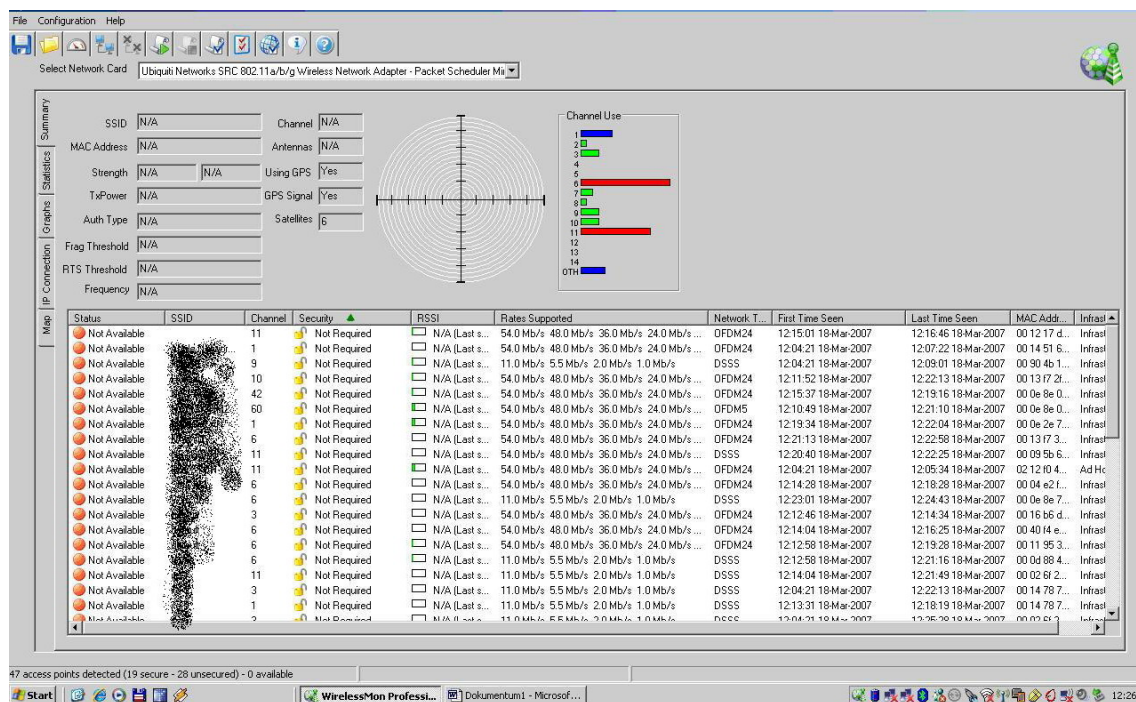
6. ábra Munka közben...
(Készítették: a szerzők)

WIFI hálózatok feltérképezése, azok eredménye

Mielőtt a fejezetbe belekezdenénk, szeretnénk kijelenteni, hogy az adatok (MAC ADDRESS-ek, SSID²²-k, stb.) kizárólag statisztika célokkal kerültek begyűjtésre, melyek a vonatkozó törvények értelmében további tárolásra, második félnek kiadásra nem kerültek.

A feltérképezéshez a Microsoft Windows alapú Wirelessmon illetve Netstumbler nevű alkalmazást használtuk. Az alábbi ábrákon a Wirelessmon alkalmazás látható, mely a wifi jelek mellett a GPS jeleket is rögzítette, azokat grafikus formában megjelenítette.

²² Service Set Identifier Egy wifi hálózat neve



7. ábra Wirelessmon működés közben
(Készítették: a szerzők)

Budapest területe

A következő állapot a 2007. április 12-i állapotot tükrözi. Az alábbi ábrán a feltérképezés GPS-szel rögzített nyomvonala látható.



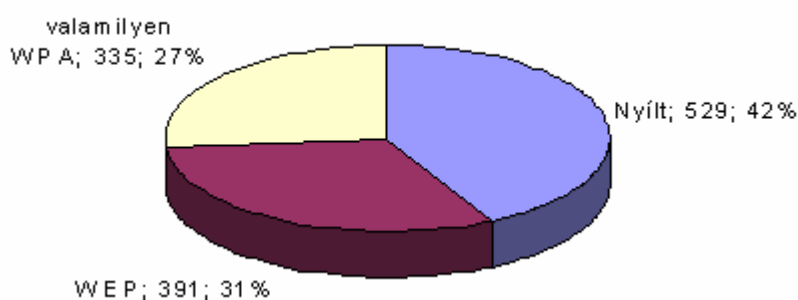
8. ábra feltérképezés nyomvonala Budapesten
(Forrás: googleearth.com)

A feltérképezés során a wifi hálózatok színes világa tárult fel. Az SSID között a hálózatsnévben telefonszámmal internet elérést kínáló hálózatoktól orvosi rendelők hálózatán keresztül, különböző rádiók, magánnyomozó irodák, politikai töltetű hálózati nevű hálózatokig szint minden megtalálható.

A csatornakihasználtság vizsgálata érdekes eredményeket hozott: vannak csatornák melyek használata fokozottabb a többinél, ezek a következők: 1-es, 6-os, 11-es, míg vannak csatornák – 4-es, 5-ös – melyeket szinte nem használnak.

A csatornakihasználtság vizsgálatának egy másik érdekes adata, hogy a 802.11b és 802.11g szabványok jóval elterjedtebbek, mint a 802.11a. Az 1255 hálózat közül csupán csak 41 használja ennek a szabványnak a csatornáit, ami az újabb, korszerűbb eszközök alacsony elterjedtségét feltételezi. Hihetetlen adat, hogy e közül a 41db 802.11a típusú hálózat közül csupán csak 2 volt titkosított miközben szinte biztos, hogy ezek a korszerű eszközök már ismerik az újabb titkosítási eljárásokat.

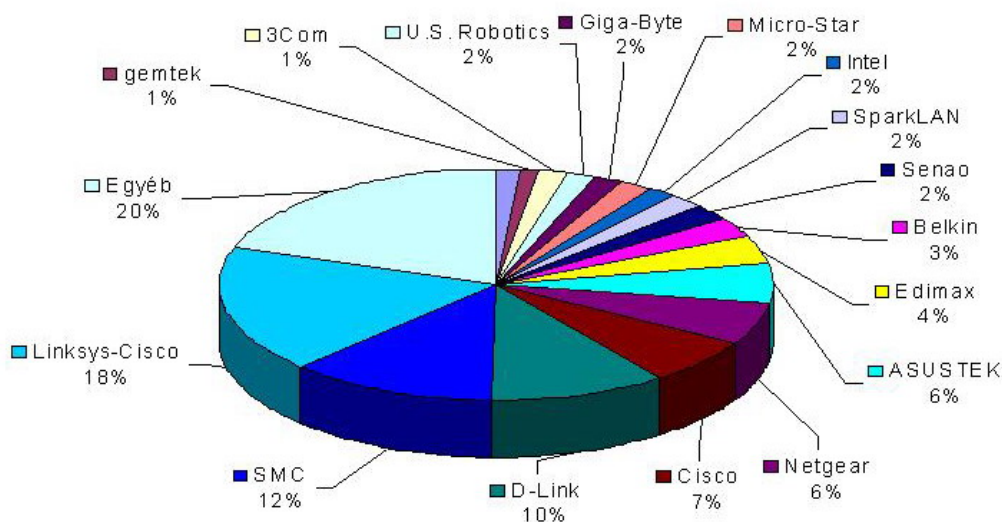
Ugyanilyen rossz a helyzet a titkosítottság általános vizsgálatakor is, az összes hálózat 42%-a teljesen nyílt volt, 31% pedig WEP alapú, mely bizonyítottan feltörhető pár óra alatt.



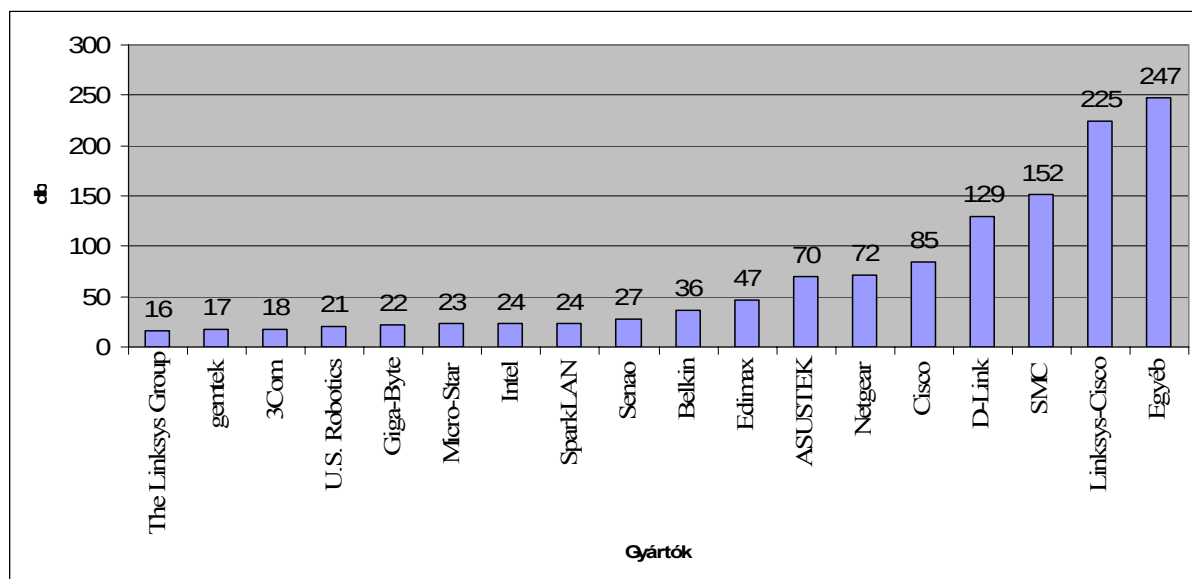
9. ábra titkosítottság megoszlása
(Készítették: a szerzők)

A sebesség tekintetében mindössze 204 AP működött kizárólag a 11 Mbps-os sebességen, a többi a nagyobb sebességekkel is elbírt, mint például a 36, vagy 54 Mbps. Ebből következtetést levonni csak óvatosan szabad, mert a korszerű eszközök is le szabályozhatóak, hogy kizárólag az alacsony sebességeket támogassák, de ilyen beállítás nem valószínű, az AP-k gyári beállítása is általában az, hogy képes minden általa támogatott sebességen dolgozni, a kliensállomás képességei és az átviteli út minősége fogja meghatározni a hálózat pillanatnyi sebességét. Ebből kiindulva úgy tűnik, hogy az első generációs, elavult eszközök lassan kihalófélben vannak.

Vizsgáltuk az eszközök gyártóit is, melyek megoszlását az alábbi grafikonok szemléltetik:



10. ábra A gyártók megoszlása I.
(Készítették: a szerzők)



11. ábra A gyártók megoszlása II.
(Készítették: a szerzők)

Mindezeket összevetve arra a következtetésre jutottunk, hogy bár sokszor lenne lehetőség magasabb színvonalú hálózat kialakítására, mégsem törekednek arra a hálózat telepítói, fenntartói.

WIFI hálózatok támadása

Ebben a fejezetben a WEP alapú hálózatok biztonsági kérdéseiről, azok kihasználásának lehetőségeiről ejtünk pár szót. Röviden bemutatjuk azokat az eszközöket, amikkel a wifi hálózatok linux alatt felderíthetők, a WEP, illetve WPA alapú hálózatok támadhatók.

A téma részletezése előtt **szeretnénk kijelenteni, hogy kizárólag saját, tesztelési célokra létrehozott hálózaton próbáltuk ki a technikákat, amelyekhez a szükséges ismereteket, software-eket az internetről szereztünk be.**

A támadás kivitelezéséhez Linux Redhat Fedora 6 operációs rendszert, valamint az alá telepített speciális software-ek, software csomagok kerültek alkalmazásra.

Aircrack-ng „software csomag”:

Legfontosabb összetevői:

- Airmo-n-g: a wifi kártya „promiscuous”, más néven „Monitor” üzemmódba való kapcsolására szolgál.
- Aireplay-ng: Többek között az elkapott, titkosított csomagok „visszajátszására”, újra küldésére való alkalmazás, mellyel IV-k generálhatók az Airodump-ng számára. Egy másik „hasznos” funkciója a már hitelesített mobil eszközök leszakítása a hálózatról, azok kényszerítése az újra autentikálásra.
- Airodump-ng: a csatornákat használó AP-k, valamint a velük asszociált mobil eszközök felderítésére használható eszköz. Számunkra legfontosabb funkciója az előző fejezetekben tárgyalt IV-k gyűjtése, file-ba történő kiírása.
- Aircrack-ng: az összegyűjtött IV-k statisztikai alapú támadására alkalmas software, mellyel a titkos WEP kulcs visszafejtése a cél.

A támadás folyamata:

1. A wifi kártyát promiscuous üzemmódba kell kapcsolni. Erre alkalmas az „*airmon-ng start wifi0*” parancs.
2. Feltérképezésre kerül a rádiós tér. Ez történhet például a Kismet vagy az Airdump programokkal: „*airodump-ng ath1*”.
3. Meg kell határozni a cél AP bssid²³-jét, az általa használt csatorna számát, a biztos siker érdekében egy, a hálózaton érvényes kliens MAC²⁴ address-ét. Ez az esetleges MAC address alapú szűrések kijátszásához hasznos. A kliens MAC address megszerzésének feltétele, hogy az eszköz hatósugarában kell lenni. Mivel ezek általában kis teljesítményű eszközök, érdemes egy nagy nyereségű antenna beszerzése.
4. El kell indítani az IV-k fogadását. Pl.: „*airodump --ivs --write adatok --channel 9 ath1*”.
5. A támadás felgyorsításának, az IV-k számának növelése érdekében „érvényes” forgalmat kell generálni. Ez történhet például „ARP request” csomagok elkapásával, azok visszajátszásával. ARP csomagok megjelenése felgyorsítható, ha leszakítjuk a hitelesítetten forgalmazó klienseszközt a hálózatról, kényszerítve azt a hálózati kapcsolat újra felépítésére. Ha ezt nem szeretnénk, akkor türelmesen várva, előbb utóbb el fogunk kapni ilyen ARP csomagot. Egy másik, hasonló megoldás lehet az érvényes forgalomgenerálásra a csomagok fabrikálása is a packetforge-ng alkalmazás segítségével.
6. Szükség esetén - bizonyos AP-k használatakor - 20 másodpercenként újra kell hitelesíteni a kapcsolatot a mobil kliens MAC address-ét használva.
7. Az Aircrack-ng program segítségével a WEP kulcs feltörése az összegyűjtött IV-k alapján.

A következő ábrán láthatóak a software-ek a támadás befejeztével. Jól látható, hogy 1 óra 30 perces hálózati forgalom generálása alatt 339794 IV került begyűjtésre, amik alapján az Aircrack-ng software 11 másodperc alatt törte fel a jelszót.

²³ Basic Service Set Identifier. Tulajdonképpen az Access Point MAC address-e.

²⁴ Media Access Controll. Hálózati eszközök egyedi azonosítója.

Airdump, gyűjti a forgalmazás során keletkező IV-eket

Airplay: ARP csomagok újrátörlesztésével forgalmat generál

Aircrack: az összegyűjtött IV-k alapján megszerzi a WEP kulcsot

12. ábra WEP törés
(Készítették: a szerzők)

ÖSSZEGZÉS: „Nem” a honvédségi használatra

Amint azt láhattuk a wifi hálózatoknak számtalan előnyös tulajdonságaik mellett, sok veszélye is lehet. Mindez adódhat szakszerűtlen telepítésből, illetve korszerűtlen eszközök alkalmazásából.

A begyűjtött SSID-ekből, következtetve nagyon sok eszköz gyári beállításokkal működik, kicsomagolás után nem került bekonfigurálásra. Rengeteg eszköz teljesen nyílt adatforgalmú, vagy elavult titkosítási eljárást használ, potenciális veszélynek kitéve a hálózat állomásait, felhasználóit.

A felsorolt hibák ellenére dolgotom nem elrettentő, hanem inkább figyelemfelkeltő céllal íródott, a wifi a civil szférában nagyon hasznos eszköze lehet hálózatok kiépítésének. A WPA alapú hálózatok megfelelő kulcs kialakításával, azok rendszeres cseréjével kielégítő védelmet nyújthatnak az alacsonyabb biztonsági szintet igénylő civil hálózatok részére.

Civilt írtunk, mert honvédségi használata nem ajánlott. Több olyan, a dolgotom eddigi részében nem tárgyalt hátránya van, melyek teljesen alkalmatlanná teszik honvédségi használatra. *Itt nem a harctéri alkalmazásra, mert arra teljesen alkalmatlanok, hanem inkább irodai használatra, az egyes nehezen bekábelezhető részek vezeték nélküli szakasszal történő kiváltására gondolunk.*

A használatukra az ellenérvek például a következők:

- nagyon könnyen felderíthetőek,
- nagyon könnyen zavarhatóak, már egy mikrohullámú sütő is bezavarhat,
- WPA használat esetén is feltörhető, bár igaz nagyon időigényes tud lenni,
- A legnagyobb problémát a folyamatosan megjelenő driver hibák jelentik. Ilyen hibát mutatott be például David Maynor és Jon Elch a 2006-os Black Hat USA konferencián. <http://www.802.11mercenary.net/~johnycsh/publications/>
<http://www.blackhat.com/html/bh-usa-06/bh-usa-06-speakers.html>