**Debreceni Egyetem**
**Informatikai Kar**

# Vezeték nélküli hálózatok biztonsági kérdései

**Témavezető:**
**Dr. Krausz Tamás**
**Egyetemi adjunktus**

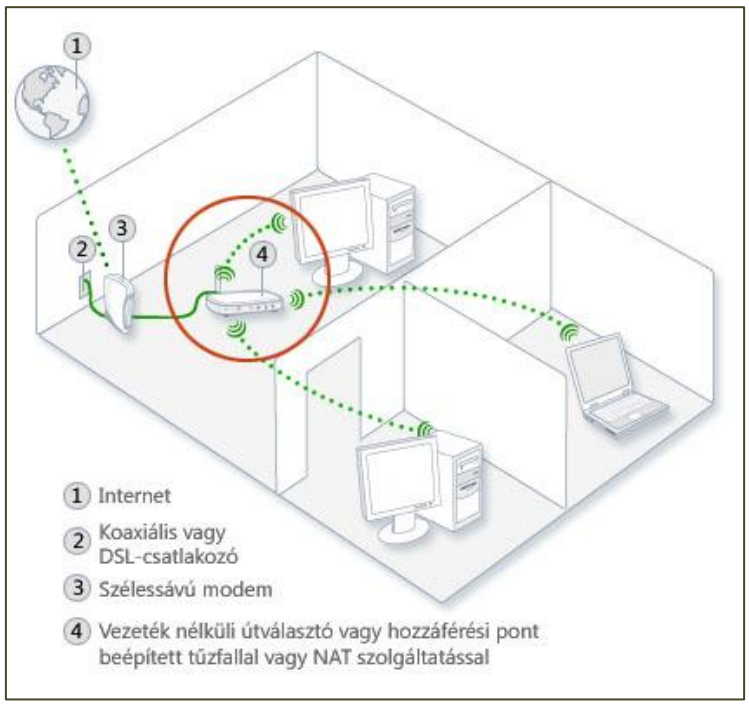
**Készítette:**
**Ungai Gusztáv**
**Mérnök informatikus**

**Debrecen**
**2011**

# Tartalomjegyzék

# 1. Bevezetés

A képesség, hogy bárki, bárkivel kommunikálhasson a világban akár nagy távolságra is egymástól, az emberiség régi álma. A Wireless (vezeték nélküli) technológia segítségével ez az álom már valóság, képesek vagyunk áthidalni nagy tereket kötöttségek nélkül. Támogatja a mobilitást, nincs szükség bonyolult kábelezési rendszerekre, olcsó és egyszerű a kiépítése, hatótávolsága és teljesítménye pedig még napjainkban is ugrásszerűen nő. Kényelmesen böngészhetünk akár a házunk kertjében is egy nyugágyban, nincs többé helyhez kötöttség asztali gépünk előtt. Vége az otthoni és munkahelyi kábelrengetegnek, a levegőt átviteli közegként használva olcsón építhetünk ki hálózatokat és könnyen konfigurálhatjuk azokat. Egy vezeték nélküli hálózatot (1. ábra) költséghatékonyabban, gyorsabban és egyszerűbben kiépíthetünk, mint egy vezetékest, főleg ha nagyobb méretű felhasználásban gondolkozunk.




1. ábra: Erőforrás megosztás vezeték nélkül

Az előnynek persze mindig van hátránya is, mivel a fizikai kapcsolatok hiánya és a rádiós csatorna jellege miatt sajnos a felhasználók több potenciális támadásnak vannak kitéve, mint vezetékes társaik. Míg egy vezetékes hálózattal rendelkező gép általában egy zárt szobában van, melynél a behatolónak hozzá kell férnie az Ethernet hubhoz, addig a vezeték nélküli hálózattal rendelkező gépnél a rádiós csatorna nyitottsága miatt a betörőnek könnyű dolga van: Hiszen egyszerűen megáll házunk vagy irodánk előtt egy lesötétített ablakú kocsival, majd egy noteszgéppel és egy Wi-Fi kártyával „belehallgat" a levegőbe. A fülelés során rengeteg felesleges, ám jó néhány igen fontos adat birtokába is juthat.

Tehát a vezeték nélküli hálózatok egyik állandó problémája megtalálni a legmegfelelőbb védelmi mechanizmust. Mivel naponta jelennek meg új szoftverek és hardverek, ezeknek a beépítése a rendszerbe más-más biztonsági kérdéseket vetnek fel. A biztonsági kérdésekkel foglalkozó szakértők, csoportok és szervezetek feladata a biztonsági rések „foltozása" a modernebb és a régebbi termékeken egyaránt. Három fontos biztonsági kérdést különböztethetünk meg, amire a hackerek törekednek: a hálózat lehallgatása, a hálózat szolgáltatásainak illetéktelen használata és a hálózat bénítása.

Dolgozatom témaválasztásakor törekedtem arra, hogy olyan témát válasszak, amely aktuális az informatikában és az átlagembert is szó szerint „behálózza" otthonában. Manapság szinte elképzelhetetlen olyan háztartás, amiben nincs jelen az Internet, mindennapunk részévé vált, nehezebben boldogulunk nélküle problémáink megoldásában. Családtagjainkkal, barátainkkal tarthatjuk a kapcsolatot, számláinkat rendezhetjük, banki ügyeinket intézhetjük el kényelmesen, otthonról. Technológia fejlettségünk azon szintjére jutottunk, hogy egy mobiltelefonnal a kezünkben akár a villamoson is tudunk böngészni a wireless technológiának köszönhetően. A kényelemnek viszont ára van, és itt nem feltétlenül a számlákra kell gondolni, hanem a felmerülő biztonsági kérdésekre. A levegő, mint éter rengeteg új felhasználási lehetőséget adott a felhasználóknak, de talán a hackereknek és crackereknek még többet! Az emberek egyszerűen kihasználhatják szomszédjaikat, akik nem is gyanakodnak, hogy más helyett fizetik Internet költségeiket. Elég kellemetlen helyzet, ha akkor derül ki mindez, amikor például a megengedett letöltési korlátot átlépi egy betolakodó.

Az elmúlt években rengeteg új technikai eszköz és fogalom jelent meg, nem túlzás azt mondani, hogy ezeknek a berendezéseknek a fejlődési lehetőségeinek száma szinte végtelen: Még nagyobb távolság áthidalása, még nagyobb sebesség elérése, még nagyobb kényelem. Ez

a három dolog az, amit egy otthoni átlagfelhasználó leginkább figyelembe vesz. Általános érvényű igazság: amikor a kényelem és az extra szolgáltatások kerülnek szembe a biztonsággal, az utóbbi általában alulmarad. Elfeledkeznek a negyedik dologról, ami a három dolgot maga mögé utasítja: a biztonságot.

Röviden szeretném megemlíteni bevezetőmben a Wi-Fi fogalmát, az OSI modell és a 802.11 kapcsolatát, mely fontos szerepet tölt be a vezeték nélküliség kialakulásában; valamint ezeknek a hálózatoknak előnyeit és hátulütőit, amit a tárgyalás részben fejtek ki bővebben a védelmi mechanizmusokon át a támadásokig. Végül bemutatom, hogyan érdemes beállítani a routert a támadások kivédésére.

## 1.1. A Wi-Fi (Wireless-Fidelity) fogalma

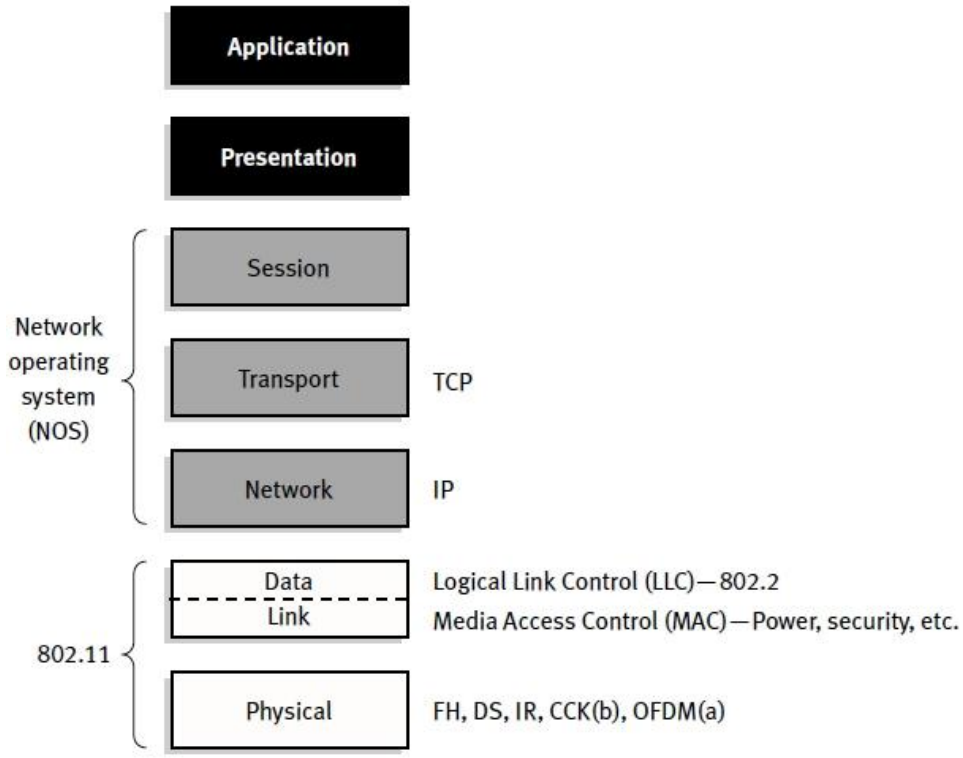
Gyakran hallhatunk a wireless jelző mellett egy másik szót is, mégpedig a Wi-Fi-t. Mit is jelent ez a hangzatos rövidítés?

Az elnevezés tulajdonképpen egy népszerű vezeték nélküli hálózati technológiát takar, amely rádióhullámokkal biztosítja a szélessávú Internet és hálózati hozzáférést számítástechnikai eszközeink számára, megkímélve minket a kábelek terhétől. Irodákban felgyorsítja és megkönnyíti a munkafolyamatot, az alkalmazottak szabadon mozoghatnak az épületben, lehetővé teszi minden felhasználó számára az Internet, adat fájlok, nyomtatók, stb. megosztását. Egyszerűen fogalmazva a Wi-Fi maga a szabadság.

A Wi-Fi Alliance szervezet konkrét meghatározása szerint Wi-Fi márkajelzésű minden olyan WLAN (vezeték nélküli helyi hálózat) termék, amely megfelel az IEEE 802.11 *(Institute of Electrical and Electronics Engineers)* vezeték nélküli adatátviteli protokoll előírásoknak. Ez tulajdonképpen egy olyan egyezmény vagy szabvány, amely leírja, hogy a hálózat résztvevői miképp tudnak egymással kommunikálni. Nagy szükség volt erre, mert kezdetben az adatkommunikációs rendszerek egyediek voltak, minden gyártó más-más megoldással rukkolt elő. Mivel a Wi-Fi szoros kapcsolatban áll az alapjául szolgáló szabvánnyal gyakran szinonimaként használják az IEEE 802.11 technológiára.

## 1.2. Az IEEE 802.11 és az OSI kapcsolata

Minden vezetékes vagy vezeték nélküli hálózatnak megfelelő protokoll szerint kell működnie. A szabályok arra vonatkoznak, hogy ki, milyen módon adhat és vehet adatot. A hálózatok működésének szemléltetéséhez leggyakrabban az OSI *(Open Systems Interconnection Basic Reference Model, 2. ábra)* modellt használják. Ezt a modellt az ISO 1977-ben dolgozta ki, és minden létező hálózatra adaptálható.




2. ábra: Az OSI Referencia Modell

A modell hét rétegből áll, ezek az ”alkalmazástól a rézdrótig” képezik a modell egy-egy részét, egymással kapcsolatban állva. A rétegek és a mögöttük lévő konkrét hardverek és szoftverek teszik lehetővé azt, hogy az adatok a fizikai rétegre eljutva minden olyan információval el legyenek látva, amelyek a nagy hálózatokban való hatékony mozgatásukhoz szükségesek. A hálózaton átjutott adat ugyanezeket a rétegeket fordítva járja be, hogy a végén a számítógépen használt alkalmazáshoz eljusson. Jelentős különbségek vannak a programokból küldött és a „dróton” mozgó adatok között - utóbbiak a különféle azonosító, hibajavító és titkosító módszerek miatt nagyobbak. Az ilyen többletadatokat hívják

*overheadnek*. Ezek nem csak az Ethernet és WLAN hálózatokban, hanem szinte minden tényleges hálózatban (pl.: GSM) és kommunikációs rendszerben (például az alaplapok buszrendszereinél) is léteznek.

Az IEEE 802.11 az OSI modell két legalsó rétegét, a fizikai és az adatkapcsolati réteget definiálja. Ahhoz, hogy a küldőt és a fogadót is azonosítani lehessen, minden számítógépnek szüksége van egy azonosítóra. A hálózati kártyák és minden hálózati eszköz rendelkezik hardveres MAC (*Media Access Control*) címmel, ám ez hossza miatt nem hatékony, csak a közvetlenül egymáshoz kapcsolódó készülékek alacsony szintű kommunikációjában vesz részt.

A MAC három hozzáférést határoz meg:

1. TDMA (időosztásos többszörös hozzáférés)
2. CSMA/CA (vivő érzékeny többszörös elérés/ütközés elkerülés)
3. Lekérdező MAC

Az adatkapcsolati rétegen belül a 802.11 LLC *(Logical Link Control)* ugyanazt a 48 bites címzésű 802.2 LLC-t használja, mint a vezetékes LAN. Ez lehetővé teszi vezeték nélküli hálózatok nagyon gyors áthidalását vezetékes hálózatok felé.

## 1.3. Vezeték nélkül, biztonságosan

Már régóta ismert fogalom a számítógépes biztonság, mivel a technika rossz kezekben fegyverként is működhet. Az IEEE 802.11 vezeték nélküli LAN szabvány (vagyis a Wi-Fi) létrejötte óta törekszik az adatok védelméért. A 802.11 korai verziója már tartalmazta a WEP *(Wired Equivalent Privacy)* biztonsági mechanizmust, melynek neve is mutatja, hogy a védelme egyenrangú egy vezetékes eszközzel, mégis hibái hamar lelepleződtek. A WEP2 ennek a kiegészítése volt, kiterjesztették a biztonsági kulcs értékét 128bit-re. Olyan hardvereken futtathatták, melyek nem voltak képesek WPA vagy WPA2-t kezelni, így a megnövelt biztonsági kulcs érték segített némileg a *„brute force”* (nyers erő) támadások

kivédésében. A WEP algoritmus egyre több felfedezett hiányosságai miatt elvetették a WEP2 elnevezést és az eredeti algoritmust.

Megszületett a WPA *(Wi-Fi Protected Access, Wi-Fi védett hozzáférés)*, mely sajnos még mindig RC4 folyamkódolót használt, mint a gyenge WEP protokoll. A WPA-val egy időben jött létre a WPA2 protokoll, ezért is van, hogy a legtöbb implementáció egyesítve tartalmazza a WPA/WPA2 protokollok kezelését. Legfőbb különbség a WPA-hoz képest az új AES (*Advanced Encryption Standard, fejlett kódolási szabvány)* kódoló használata a régi RC4 algoritmus helyett. A WPA-t egyelőre nehézkesen, de a WEP protokollt viszonylag egyszerűen kezelhető szoftverekkel is fel lehet törni, mégis a routerek a mai napig támogatják ezt a gyenge protokollt a régi kliensek kompatibilitása miatt. Az adok-kapok játék folyamatosan fennáll a hackerek és a tervezők között: a tervezők előrukkolnak egy új biztonsági szabvánnyal, melynek hibáira a hackerek derítenek fényt. Jön egy újabb szabvány, ami a tervezők szerint elvileg szintén feltörhetetlen, és a játék folytatódik...

Egy másik szempont szerint is vizsgálhatjuk a biztonságot, vagyis okoz-e egészségügyi károsodást a sugárzás? A mobiltelefonok elterjedésekor is nagy port kavart ez a kérdés, a mai napig nem tisztázódott, hogy valós-e ez a veszélylehetőség. Az ISM-sávban 100 mW a megengedett kisugárzott teljesítmény, tehát korlátozott. Jelenleg a Wi-Fi esetében szintén nincs bizonyíték arra vonatkozóan, hogy bármiféle egészségkárosító hatása lenne.

## 1.4 Biztonsági tévhitek

***Nincs semmi olyanom, amit egy internetes bűnöző akarhat:***

A hétköznapi felhasználók általában úgy gondolják, az ő gépükön nincsen semmi értékes mások számára, így nincs is értelme nagy ügyet csinálni a védekezésből. Ezzel az elmélettel három probléma is van. Először is, sok támadó nem adatokra vadászik, hanem „csak” át akarja venni az uralmat a gépünk felett, hogy egy bothálózat részeként más gépeket, nagyobb oldalakat támadjon meg vele, vagy éppen levélszemetet küldjön rajta keresztül. Másodszor, a saját magunknak olyan triviális adatok, mint a teljes nevünk vagy lakcímünk is elég lehet arra, hogy egy hacker felhasználja azokat személyiséglopásra. Harmadrészt pedig jó

pár támadás automatikusan, programok segítségével történik, amelyek megtámadnak bármilyen rendszert, amelyik sérülékenynek tűnik, és nem vizsgálják, van-e bármi hasznos adat az adott gépen.

***A hálózati eszközömön van tűzfal, ezért a PC-m tökéletesen védett:***

Egy tűzfal remek gát lehet véletlenszerű támadások elhárítására, és számos dolog ellen hatékonyan védi a felhasználó gépét, de a támadók régóta rájöttek, hogy a leggyorsabb út a védelmen keresztül azoknak a portoknak a kihasználása, amelyeken a hagyományos, nem veszélyesnek tartott adatforgalom zajlik. Alapbeállításként az útválasztó tűzfala nem szűri az e-mail-és böngészőforgalmat, és kevesen tudják, hogy hogyan is kell átállítani ezeket a feltételeket, mit kellene blokkolni és mit átengedni feltétel nélkül. Ráadásul a mai támadások már webalapúak, vagy adathalász-félrevezetésen alapulnak, amelynek az a lényege, hogy önszántunkból látogassunk el egy veszélyes oldalra. Márpedig ez ellen a tűzfal nem véd.

***Csak akkor vagyok veszélyben, ha Windowst használok:***

A Microsoftnak kétségkívül nagy rész jutott az utóbbi években biztonsági problémáiból, de ez nem jelenti azt, hogy a többi operációs rendszer immunis lenne a támadásokra. A piaci részesedése miatt a Windows a legnagyobb célpont, de a Mac OS és Linux is rejt biztonsági réseket, csak ezeket ritkán éri meg kihasználni, vagy éppen energiát fektetni a felfedésükbe, hiszen kevesebb felhasználót lehet velük átejteni számszerűen. Az a trend figyelhető meg, hogy a bűnözők is inkább olyan cross-platform alkalmazások sérülékenységeinek kihasználására törekednek, mint például az Adobe Reader, amelyekkel mindenki célponttá válhat, függetlenül attól, hogy milyen operációs rendszeren használja azt.

## 1.5 Vezeték nélkül, kényelmesen

Mint már említettem, napjaink meghatározó tényezőjévé vált az Internet, és annak folyamatos elérhetősége bárhol és bármikor. Vége már a csak vezetékes internet-szolgáltatás és vezetékes helyi hálózatok korának: manapság egyre jobban terjednek az otthoni és cégen belüli vezeték nélküli hálózatok. Tény, hogy sebességük még nem éri el a vezetékesét, ahol már a gigabites átvitel sem számít ritkaságnak. Ezzel szemben a 802.11g zsinór nélküli szabvány is csak 54 megabitre képes (ez egyébként egy kisebb irodának bőven elég). A Wi-Fi legnagyobb hátulütője, hogy nehéz – de nem lehetetlen – biztonságosan üzemeltetni. A légtérben haladó rádióhullámokhoz hasonlóan az irányukat ugyanis nem tudjuk megszabni, ezért könnyen „lehallgathatók". Ettől függetlenül ma már nincs olyan hordozható számítógép, amiben ne lenne Wi-Fi-eléréshez szükséges eszköz, legyen az notebook, PDA vagy okostelefon. Egyre több cég, kávézó, szálloda, gyorsétterem és oktatási intézmény rendelkezik úgynevezett „forróponttal" (*hot spot*), amelyen keresztül vezeték nélküli hálózathoz csatlakozhatunk. Ez természetesen csak néhány példa, szélsőséges alkalmazási lehetőségeként érdemes megemlíteni, hogy az Intel a Barneo sarkköri táborban, az Északi-sarkon is felállított egy elérési pontot kísérletképpen.

## 1.6 Wardriving

A vezeték nélküli hálózatok elterjedésének következtében mondhatni kialakult egy új hobbi. Én ezt úgy nevezném el, hogy „Wi-Fi vadászat". Az emberek akkora érdeklődést mutatnak eme új sport iránt, hogy vezeték nélküli eszközökkel, és GPS-szel „felfegyverkezve" körbejárják a várost, és feltérképezik egy adott területen elérhető Wi-fi hálózatokat. Ez a *wardriving* (gépjárművel), illetve *warchalking* (gyalog). Az elnevezés még a '80-as évek Amerikájának koldusaitól eredeztethető. A hajléktalanok krétajeleket hagytak társaiknak a járdán, azokon a helyeken, ahol adományokra számíthattak, vagy épp ellenkezőleg, amelyeket ajánlott volt nagy ívben elkerülni, mondjuk mogorva emberek, házőrző kutya miatt. Ezt hívták ők „warchalkingnak" (chalk = kréta). Kezdetben a Wi-Fi

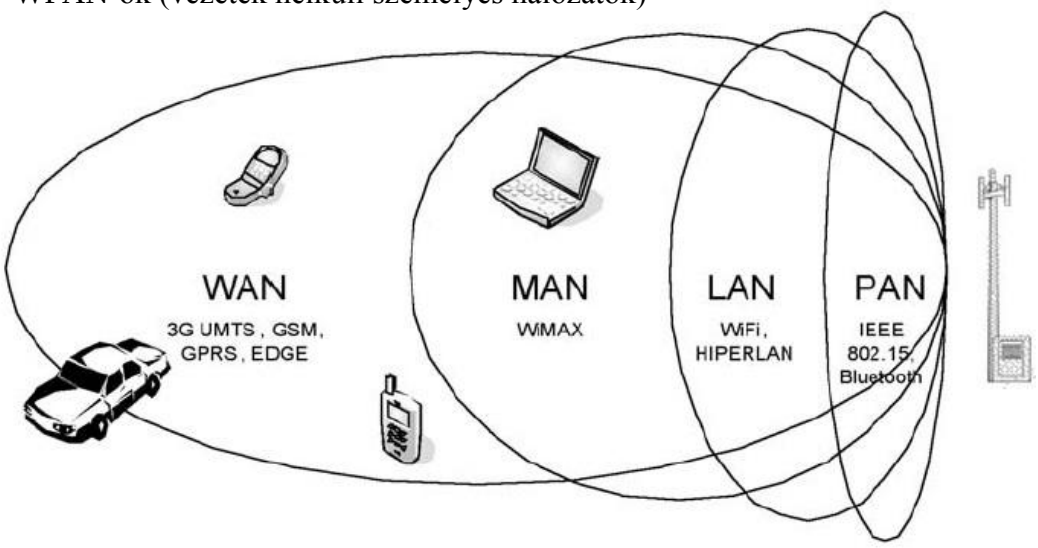
betolakodók szintén krétával jelezték egymásnak, ha valahol nyitott hálózatot találtak, manapság ezekről már inkább e célra fenntartott weboldalakon számolnak be GPS-adatokkal és térképpel. A wardriving mégsem jelent egyet a támadható hálózatok feltörésével. Bár elég radikális a módszer, mégis inkább egyfajta rámutatás, mennyivel többet kéne foglalkozniuk a felhasználóknak a biztonságukért.

# 2. Tárgyalás

## 2.1. Wireless hálózatok méretük szerinti csoportosítása

A vezeték nélküli hálózatok hasonlóan a vezetékes hálózatokhoz szintén csoportosíthatóak kiterjedésük szerint (3. ábra):

- WWAN-ok (nagy kiterjedésű vezeték nélküli hálózatok)
- WMAN-ok (nagyvárosi vezeték nélküli hálózatok)
- WLAN-ok (helyi vezeték nélküli hálózatok)
- WPAN-ok (vezeték nélküli személyes hálózatok)

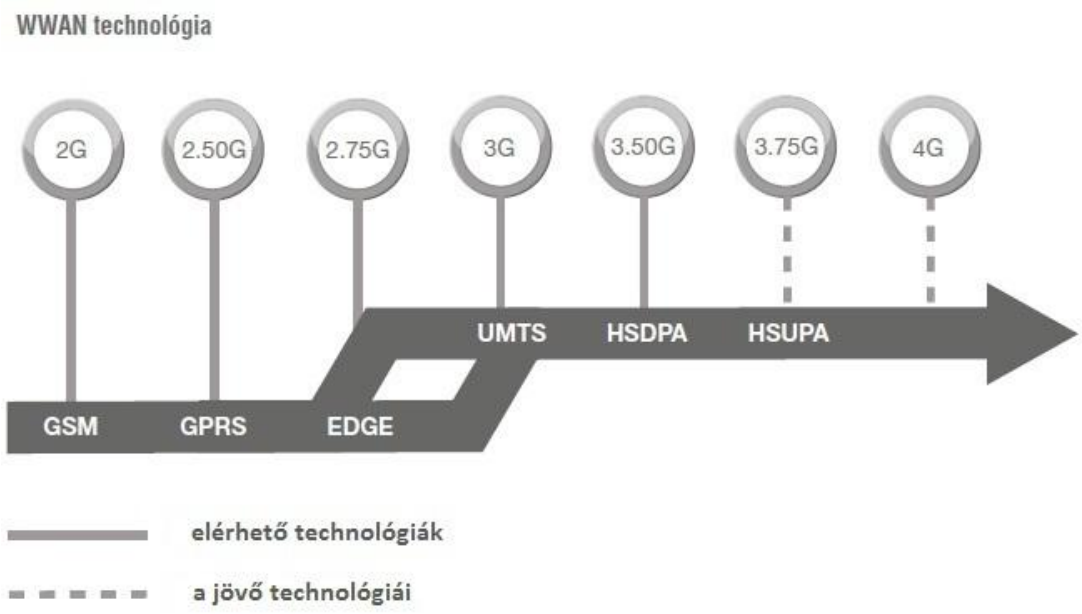



3. ábra: Wireless hálózatok kiterjedéseinek szemléltetése

### 2.1.1. WWAN (Wireless Wide Area Network)

Olyan vállalkozások számára, ahol a beosztottaknak sokat kell utazniuk munkájukból kifolyólag, elengedhetetlen ez a fajta wireless megoldás. Ezáltal a cég dolgozói bárhol és bármikor, akár utazás közben is hozzáférhetnek az Internethez és a vállalat adatbázisához, növelve ezzel munkájuk hatékonyságát. Hazánkban viszont még ma is sokaknak szokatlan és új lehetőség vonaton, autóban, buszon az internethez való hozzáférhetőség. A megoldás pedig kézenfekvő, a mobilok által is használt hálózat celláit kihasználva, nagy területen, gyors és egyúttal biztonságos kapcsolatot nyerhetünk, mely lehet GPRS alapú, vagy valamilyen harmadik generációs hálózaton üzemelő csomagkapcsolt adatszolgáltatás.

A WWAN előnye a WLAN technológiával szemben a még nagyobb szabadság lehetősége. Míg a WLAN lefedettsége otthonunkban és irodánkban meghatározott, addig a mobilhálózat akár egy egész országot is lefedhet. Összesen 7 mobil-adatátviteli lehetőséget tartanak számon (4. ábra):




4. ábra: Mai és jövőbeli WWAN technológiák

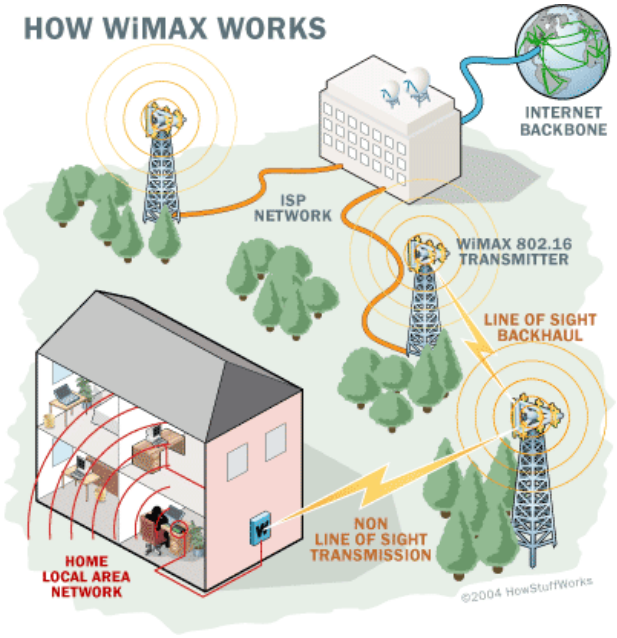
- 2G – GSM *(Global System for Mobile Communications)*
- 2.5G – GPRS *(General Packet Radio Services)*
- 2.75G – EDGE *(Enhanced Data GSM Environment)*
- 3G – UMTS *(Universal Mobile Telecommunications Service)*
- 3.5G – HSDPA *(High Speed Downlink Packet Access)*
- 3.75G – HSUPA *(High-Speed Uplink Packet Access)*
- 4G

Ezek közül a leginkább széles körben használt a 3G és a 3,5 G WWAN generáció. Ezeket a megoldásokat válthatja fel a jövőben a 3.75G HSUPA és a 4G technológia.

Több mint 20 év után, 2009-ben feltörték a GSM technológiát. Igaz, hogy a biztonságért felelős A5/1 titkosító algoritmus csak 64 bites bináris kódolású, mégis a GSM-nél a titkosítások 80%-áért ez felelős. Ha például egy hacker meg is szerezné a titkosítási kulcsot, az még önmagában nem elegendő a lehallgatáshoz. Ki kell választania a bázisállomáson folyamatban lévő több ezer hívás közül az aktuális digitális jelfolyamot. Ez nem egyszerű feladat, mivel a jelek 60 frekvencián rezegnek a szolgáltatók miatt, akik így használják ki a rendelkezésükre álló teljes frekvenciatartományt. Ezzel szemben a 3G hálózatok már erősebb, 128 bites titkosítást alkalmaznak, melyre feltörést még nem regisztráltak.

### 2.1.2. WMAN (Wireless Metropolitan Area Network)

A hotspotok (hozzáférési pont) kapcsán felmerül a kérdés: nem lehetne-e nagyban is megcsinálni? Itt jön a képbe az IEEE 802.16, azaz a WiMAX (*Worldwide Interoperability for Microwave Access, 5. ábra).* A WiMAX a Wi-Fi nagytestvére is lehetne, azonban annál jóval fejlettebb.




5. ábra: A WiMAX működése a szolgáltatótól az előfizetőig

Hatékonyabb adattitkosítást alkalmaz, valamint 2–11 gigahertzes frekvenciasávban működik, szemben a Wi-Fi 2,4 gigahertzes sávjával. A technológia elvben 50 kilométeres körben 70 megabit/másodperc sebességet biztosít, a bázisállomásra való közvetlen rálátás nélkül. A gyakorlat azonban azt mutatja, hogy 3–10 kilométeres körben körülbelül 40 megabit/másodperc csatornánkénti átviteli sebesség érhető el. Az üzletekben is kapható, azaz mindenki számára hozzáférhető, hordozható rendszerek várhatóan 15 Mbps átvitelre lesznek képesek három kilométeres körben. Ez a megoldás tehát ígéretes technológia a jelenlegi WLAN felhasználási területein, mivel hosszabb hatótávolságot, nagyobb kapacitást, valamint jobb QoS *(Quality of Service-szolgáltatás minőség)* és biztonsági megoldásokat kínál.

A WiMAX technológiával könnyedén le lehet fedni egy várost, s ez mindenképpen olcsóbb, mint réz- vagy optikai kábelt fektetni. Egyelőre azonban nem kell számolni a WiMAX gyors elterjedésével, csak az úgynevezett „Last-mile” (utolsó mérföld) típusú felhasználással. Ennek az a gyakorlati lényege, hogy szélessávú interneteléréssel még nem – vagy csak gyéren – ellátott településeken is elérhetővé tegyék a szolgáltatást mindenki számára. Kiépítése jóval gazdaságosabb, mint a rézalapú DSL-vonalé, főleg ha utóbbit csak kevés felhasználó veszi igénybe. Egyesek úgy gondolják, hogy az új technológia még a jelenleg használt mobiltelefon-hálózatokat is leválthatja, erre azonban a közeljövőben nem látni reális esélyt, hisz a szolgáltatók rengeteg pénzt öltek a megfelelő lefedettség

létrehozásába, nem valószínű, hogy egyszeriben változtatnának bármit is a már kiépült rendszeren.

### 2.1.3. WLAN (Wireless Lan Area Network)

A notebookok rohamos terjedése, megközelíthetetlen helyekre történő hálózat kiépítése, autóutak feletti kábelezési rendszerek kiépítésének bonyolultságai és az esztétikai problémák megkövetelték egy új átviteli közeg bevezetését. Ezen problémák hatására 1997-ben indult világhódító útjára a 802.11 szabvány, amely attól kezdve nagy fejlődéseken ment át és a 2000. év után terjedt el széles körben. Bevezetőmben részleteztem, hogy ez a protokoll az OSI modell két legalsó rétegét, a fizikai és az adatkapcsolati réteget definiálja. A WLAN-hoz szükség van egy fix csatlakozási pontra, amely segítségével az összes WLAN hálózatban lévő vezeték nélküli egység a vezetékes hálózatra kapcsolható. Szórt spektrummal vagy ortogonális frekvencia-osztásos multiplexálás technológiával a levegőt használva éterként lehetőséget ad a közeli számítógépek összekapcsolódására vagy önálló ad-hoc hálózatok létesítésére. Celluláris architektúrája a GSM rendszerhez hasonlóan cellákra van osztva. Ezeket a cellákat (BSS) hozzáférési pontok irányítják (*Access Point* vagy hotspot, röviden AP). A kábeles megoldásoknál olcsóbbnak bizonyult a WLAN hálózatok kiépítése, a kevesebb hálózati eszköznek köszönhetően. Alkalmazása nagyon népszerű oktatási intézményekben, kávézókban, repülőtereken, irodaépületekben és otthonunkban.

Alapvetően kétféle WLAN hálózati topológiát különböztethetünk meg:

- *Ad-hoc mód:* Hozzáférési pont nélkül működtethető ez a fajta hálózati topológia, melyben minden eszköz azonos szerepet tölt be. Legtipikusabb felhasználása az, amikor két számítógépet bázis nélkül kötünk össze, ez az úgynevezett peer-to-peer (P2P) kapcsolat, mely az ad-hoc módban valósul meg. Könnyű beállítani, nem szükséges hozzá külső eszköz vagy valamilyen előre telepített infrastruktúra.
- *Csillag topológia:* Egy hozzáférési pont segítségével működik. Az egyik mobil csomópont elküldi az információt a központi állomásnak, ami azt a célcsomópont felé továbbítja, ez az elrendezés az infrastruktúrahálózat (6. ábra).


6. ábra: Infrastruktúra hálózati topológia. Eszközeinket még hatékonyabban használhatjuk

### *2.1.3.1. IEEE 802.11*

1997-ben, az IEEE (Institute of Electrical and Electronics Engineers) megalkotta az első WLAN szabványt. Sajnos a 802.11 a legtöbb alkalmazáshoz túl lassú volt, mivel maximális adatátviteli sebessége csupán 2 Mbps volt. Fizikai réteg szerint három lehetőséget határoz meg, egyet az infravörös tartományban, kettőt pedig a szórt spektrumú sávban, a szabad 2.4GHz-es ISM tartományban:

- *IR:* infravörös, maximum 2 Mbps, a gyakorlatban nem terjedt el.
- *FHSS (Frequency Hopping Spread Spectrum):* Frekvenciaugrásos szórt spektrumú.
- *DSSS (Direct Sequence Spread Spectrum):* Az ilyen kódolásnál minden átvinni kívánt bitet egy redundáns bitmintával helyettesítenek. Minél hosszabb ez a bitminta, annál nagyobb a valószínűsége, hogy az átviteli torzulások ellenére az eredeti jel helyreállítható. A legtöbb vezeték nélküli LAN eszközöket gyártó cég a DSSS eljárást választotta a kódoláshoz.

### *2.1.3.2. IEEE 802.11b*

1999-ben továbbfejlesztették a 802.11-t, ez lett a 802.11b specifikáció. Támogatja a 11 Mbps sebességet, de a távolság miatt bekövetkező ún. sebesség-visszaesési ráta 5.5, 2, és 1 Mbps lehet. Ugyanazt a szabályozatlan rádió frekvenciát használja (2,4 GHz), mint az eredeti 802.11 és DSSS valamint *CCK (Complementary Code Keying: komplemens kódú kulcs)* modulációt használ. Mivel a jel szabályozatlan, zavarhatják a hasonló frekvenciát használó eszközök, mint például a mobiltelefonok walkie-talkie, Bluetooth- eszközök, vezeték nélküli kamerák, sőt még a mikrohullámú sütő is - bár megfelelő elhelyezéssel ez a probléma kiküszöbölhető. Negatívuma még, hogy a 802.11b WEP hálózati biztonsági megoldása sem a legmegbízhatóbb. Mégis relatív nagy sebessége és viszonylag olcsó ára miatt nagyon gyorsan elterjedt.

### *2.1.3.3. IEEE 802.11a*

Amíg a 802.11b fejlesztési stádiumban volt, addig az IEEE létrehozott egy második kiterjesztetést az eredeti 802.11 alapján. Egyesek úgy vélték, mivel a 802.11b népszerűsége sokkal nagyobb volt, hogy a 802.11a szabványt később hozták létre. Valójában a két szabvány egy időben készült el, de a magasabb költségek miatt a 802.11a-t inkább irodai hálózatokba szánták, az olcsóbb 802.11b-t pedig otthoni célokra használták.

A 802.11a az *OFDM (Orthogonal Frequency Division Multiplexing-ortogonális frekvencia-osztásos multiplexelés)* révén támogatja akár az 54 Mbps sávszélességet. Az 5 GHz-es frekvenciatartománynak köszönhetően csökkent az interferencia, mivel ez a lehetőség 13 interferenciamentes csatornát kínál és elég kevés eszköz dolgozik ebben a tartományban. A vezetékes világgal egy nagyságrendben lévő adatátviteli sebesség ellenére a 802.11a rendszerek mind a mai napig nem terjedtek el. Ennek egyik oka az 5 GHz-es tartomány korlátozott hozzáférhetősége a katonai radarok hasonló frekvenciái miatt. Másik óriási hátránya, hogy ezek az eszközök nem kompatibilisek a 802.11b-vel, mivel azok más frekvencián működnek. Ezen hibákból tanulva 2003 folyamán megjelent a 802.11g szabvány, amely az OFDM moduláció alkalmazásával a 2,4 GHz-s sávban is eléri az 54 Mbps sebességet, ráadásul kompatibilis a 802.11b-vel.

### *2.1.3.4. IEEE 802.11g*

Felesleges vita tárgya lenne, hogy az előző két szabvány közül melyik a jobb, mivel mindkettőnek megvan a maga előnye és hátránya. 2003-ban bemutattak egy új szabványt, mely ötvözte az elődök jó tulajdonságait, bár még mindig maradtak hiányosságok.

A 802.11g egy nagysebességű fizikai réteget *(PHY)* jelent, és a 802.11b szabvány kibővített verziója, teljes mértékben kompatibilis vele. A mai routerek a „b" és „g" szabványt egyaránt támogatják. A kompatibilitás a 2.4 GHz-es sáv és a CCK modulációs séma alkalmazásával valósul meg. A nagy sebesség kulcsa a már 802.11a szabványnál bevált OFDM eljárás. A 802.11g hátránya megegyezik a „b" szabvánnyal, mivel csak 3 zavarmentes csatornát kínál. A 802.11g szabvány maximális adatátviteli sebessége 54Mbit/s, viszont a távolság növekedésével lényegesen romlik a hatásfoka.

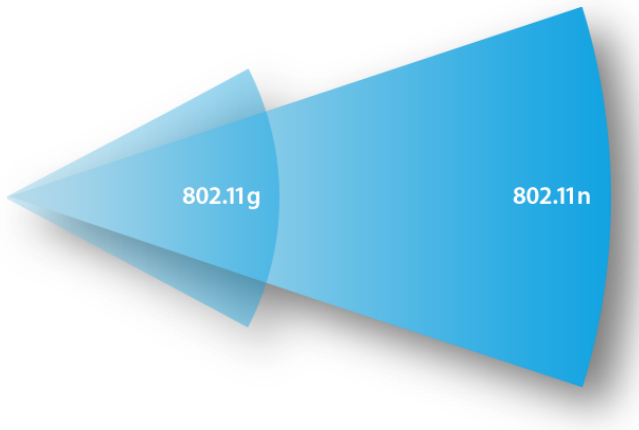
Vegyes üzemmódú védelem (Mixed mode) esetén a „g" eszközök sebességét jelentősen befolyásolja a használt védelmi mechanizmus *(RTS/CTS vagy CTS-to-self)*. Ez a beállítás az adatütközések elkerülésére szolgál vegyes 802.11b / 802.11g környezetekben. Ha a gépek valamilyen okból kifolyólag nem hallják egymást, akkor érdemes használni az RTS/CTS jelpárt. A CTS mindenkinek (CTS-to-self) engedélyezésével javítani lehet az átbocsátást az olyan környezetekben, ahol az eszközök túlságosan közel vannak egymáshoz és hallják egymást.

### *2.1.3.5. IEEE 802.11n*

A 802.11n szabvány véglegesítéséhez hét év kellett, bár figyelembe véve komplexitását nem tűnik soknak, de mégis megkéstek vele, mivel ma már még nagyobb sávszélesség igény figyelhető meg. A végleges változat megjelenésig úgynevezett nem ratifikált Draft-N eszközök terjedtek el a piacon, amelyek már 2.0-ás változatnál tartanak. A Wi-Fi Alliance végül elszánta magát, és 2009.szeptember 11-én véglegesítette a 802.11n szabványt, amit akár mérföldkőnek is nevezhetnénk, ám a felhasználók számára nem sok minden fog változni. Kevésbé valószínűsíthető, hogy a most bemutatott ratifikált változat ezekhez az eszközökhöz képest hozhat még módosításokat, mivel csupán néhány elméleti probléma akadályozta meg a véglegesítést, például a 2,4 gigahertzes sávon a 40 megahertzes sávszélesség állítólag zavarhatja a hagyományos (20Mhz-s sávszélességű) 2,4 gigahertzen

működő eszközöket. A funkciókkal viszont nem volt gond, tehát tudás terén nem lesz változás. A piac már bőven megérett egy jobb, gyorsabb szabványra, hiszen a „b” és „g” szabvány már elavult, a sebességük pedig kevés a mai igényeket és állományméreteket tekintve. A Draft-N 2.0 eszközök folyamatos árcsökkenése szempontjából megkérdőjelezhető a 802.11g létjogosultsága.

Az „n” szabvány elméleti átviteli sebessége 300 Mbps, azaz 37,5 megabájt, de természetesen a gyakorlatban ez nem teljesíthető. Tapasztalatok alapján az új eszközök akár 80-90 megabites átviteli sebességre képesek, ami sokkal jobb, mint a 802.11g-nél mérhető maximális 11-15 megabit - 54 helyett. A nagyobb hatótávolságát és sávszélességét (7. ábra) az adatátviteli csatornák párhuzamos használatával érték el, mely lényegében a MIMO (*Multiple Input, Multiple Output)* technológiát takarja, amelyhez már nem két, hanem legalább három antenna szükségeltetik, így egy adatcsatorna helyett három csatornán képes adni és kettőn venni adatokat. Ezáltal csökkenthető a visszaverődésből eredő jelgyengülés és megszünteti a házon belüli jelmentes zónákat. Próbálkoztak a „g”-s eszközöknél is három antenna alkalmazásával, mégis a 802.11n szabvány szükségeltetett ahhoz, hogy tökéletesen működjön a MIMO.




7. ábra: A „g” és az „n” szabvány elvi lefedettség különbségeinek szemléltetése

A 802.11n eszközök nem csak sebesség és lefedettség szempontjából fejlettek, hanem abban is, hogy az úgynevezett *Dual Band (hibrid)*, azaz kétsávos típusok a 2,4 gigahertzes sáv mellett a jóval kevésbé leterhelt 5 gigahertzen is képesek sugározni. Ez a tény kompatibilitást teremt a 802.11a-val (ami gyakorlatilag ugyanarra képes, mint a 802.11g, csak 5 gigahertzen), viszont annál jóval gyorsabban. Főleg akkor érdemes használni, ha túl sok 2,4 gigahertzes

sávot használó eszköz van környezetünkben, ami miatt a hálózat használhatósága korlátozottá válik. A rádiófrekvenciás és elektronikus eszközök mind csökkentik a 2,4 gigahertzes vezeték nélküli hálózat teljesítményét, ezért az 5 gigahertzes sáv reális és könnyen elérhető alternatívát kínál a sűrűn lakott környezetben.

A *Quad Band* eszközök gyakorlatilag megegyeznek a kétsávos Dual Band eszközökkel, de ezek szimultán képesek mindkét frekvencián sugározni. A Quad Band előnye, hogy nem kell a router menüjében válogatni a sávok között és újraindítani az infrastruktúrát (aminek következtében az aktív kliensek nemcsak hogy leszakadnak a hálózatról, de az 5 gigahertzet nem támogató eszközök ezt követően nem is képesek rá visszacsatlakozni), hanem az adott gépen elegendő a másik frekvenciára kapcsolódni. Az éterben a két sávot külön *SSID* azonosítja, ezért egy Wi-Fi - klienssel egyszerre csak az egyik frekvencián sugárzott hálózatra csatlakozhatunk. Ráadásul ahhoz, hogy mindkét sáv előnyeit ki tudjuk használni, olyan hardver szükséges, ami a 802.11a/n szabvánnyal is kompatibilis, ennek hiányában csak a 2,4 gigahertzes sáv használható.

Érdekes, hogy az IEEE 802.11n szabványú routerek már nem támogatják a WEP-titkosítást, úgy tűnik szakítottak a hagyományokkal, és ez egy pozitív lépés a biztonságosabb hálózatok érdekében. A WEP valójában már a szabvány leírásában sem szerepel, ami a gyakorlatban annyit jelent, hogy WEP-titkosítást használva útválasztónk 802.11b/g módban fog működni. Érdemesebb WPA-t használni bonyolult kulccsal és további biztonsági intézkedésekkel, mint például tűzfal beállítása, Mac-cím szűrés, IP korlátozás, stb. Amennyiben régebbi IEEE 802.11b/g szabványú eszközeinket szeretnénk a hálózaton használni, WEP2 AES-CCMP titkosítása ajánlott. Ezekről a beállításokról, és titkosításokról később részletesen írok.

### *2.1.3.6. IEEE 802.11y*

Az IEEE 802.11y egy 2008 novemberében kiadott protokoll, ami OFDM modulációt használ 3650 és 3700 MHz közötti vivőkön. Leginkább az Egyesült Államokban terjedt el. Maximális sebessége 54 Mbps lehet, vagyis ugyanakkora, mint az „a” vagy a „g” szabvány esetében, azonban az adóteljesítmény jóval nagyobb, szabadtéren akár 5 km-es hatótávolság elérését is lehetővé teszi. Valószínűleg kevesen fogják ezt otthoni célokra használni.

A WLAN hálózatok legismertebb szabványai és fontosabb jellemzői táblázatban összefoglalva:

1. táblázat: IEEE szabványgenerációk összehasonlítása

| IEEE szabvány | Megjelenés | Működési frekvencia (GHz) | Bitsebesség (Mbps) | Hatótávolság beltéren (méter) | Hatótávolság kültéren (méter) | Moduláció |
|---|---|---|---|---|---|---|
| 802.11 | 1997 | 2,4 vagy IR | 2 | ~20 | ~100 | PSK (FHSS vagy DSSS) |
| 802.11a | 1999 | ~5 | 54 (24, 12, 6) | ~35 | ~120 | OFDM |
| 802.11b | 1999 | 2,4-2,5 | 11 (5.5, 2, 1) | ~38 | ~140 | CCK (DSSS) |
| 802.11g | 2003 | 2,4-2,5 | 20-54 | ~38 | ~140 | OFDM |
| 802.11n | 2008 draft, 2009 végleges | 2,4 vagy 5 | 74-300 | ~70 | ~250 | OFDM (DSSS) |
| 802.11y | 2008 | 3,7 | 23-54 | ~50 | ~5000 | OFDM |

Az otthoni-kisirodai vezeték nélküli hálózatok megtervezése során számít ugyan az eszközök áteresztőképessége, egymással való kompatibilitása, de a fő szempontok közül továbbra is az ár lesz az egyik meghatározó. Az igazán felszerelt, egy átlagos felhasználó számára javarészt kihasználatlan szolgáltatásokkal rendelkező útválasztók, adapterek még mindig nagyon drágák, így továbbra óriási igény van az olcsó, de könnyen konfigurálható és megbízható eszközökre.

### 2.1.4. WPAN (Wireless Personal Area Network)

Ez a technológia lehetőséget ad a felhasználóknak személyes működési környezetükben (POS-Personal Operating Space), hogy eszközeik (pl. PDA-k, mobiltelefonok és laptopok) ad hoc módban kommunikálhassanak egymással. Kis hatótávolságuk miatt sajnos az eszközöknek igen közel kell lenniük egymáshoz a kommunikáció közben. Ez változó távolság, de átlagosan legfeljebb 10 méter.

Egyik ilyen WPAN átviteli lehetőség a *Bluetooth,* ami az *IEEE 802.15* szabványra épül. Ideális esetben, ha egy mobiltelefon és egy PC felismeri így egymást, úgy kommunikálhatnak, mintha kábellel lennének összekötve. Egy másik fontos jellemzője az a képesség, hogy szelektíven képes kizárni más eszközöket, megakadályozza a szükségtelen zavarást, vagy információkhoz való jogosulatlan hozzáférést. Alternatív lehetőségként, nagyon kis távolságon belül (egy méter vagy kevesebb) a felhasználók infravörös kapcsolatot is használhatnak.

## 2.2. Biztonsági mechanizmusok ismertetése

Ezek olyan eljárási módszerek vagy megoldási elvek, amik azt a célt szolgálják, hogy egy vagy több biztonsági követelményt teljesítsenek. A védelmi intézkedések sorát biztonsági szabványok határozzák meg. Ezeket az eljárásokat a gyártó cégek beépítik a hardver és szoftver termékeikbe és így szolgáltatják a felhasználók részére. A megvalósított védelemnek zártnak, teljes körűnek, a kockázatokkal arányosnak és időben folyamatosan biztosítottnak kell lennie.

### 2.2.1. Nyílt és titkosított hálózatok

Vezeték nélküli hálózatainkat védelem szempontjából két csoportba sorolhatjuk be: *nyílt* vagy *titkosított hálózatok*.

Az eddig részletezett WLAN szabványok egytől-egyig támogatják mindkét lehetőséget, viszont számolni kell azzal, hogy némely hálózati eszköz nem ismeri fel az újabb titkosítást, leginkább a régebbiek, amelyek kevesebb védelmi lehetőséget kínálnak. Ilyen esetben egy lehetséges megoldás, hogy nyílt hálózatot használunk, ami azért veszélyes, mert bárki könnyedén csatlakozhat rá azonosítás és jelszó megadása nélkül, ráadásul az adatok szöveges formában továbbítódnak *(plain text)*. Erre a módszerre részletesen kitérek a támadási lehetőségeknél. A betolakodó könnyedén képes olvasni az átvitt adatokat, mint

például jelszavakat. Ez megvalósulhat az úgynevezett *sniffing* technikával, melynek lényege a hálózati forgalom lehallgatása.

A következő esetekben lehetséges, hogy még valaki nyílt hálózatot használ:

- Legritkább az az eset, hogy az eszköz nem támogatja az újabb titkosításokat.
- Leggyakoribb eset az, hogy a felhasználók a gyári alapértelmezett (default) beállításokat nem változtatták meg.
- 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. A captive portal tulajdonképpen egy hotspot hozzáférés. A felhasználónak először ehhez a nyílt SSID-re kell csatlakoznia, ekkor a böngészőben még csak a vállalat portálja jelenik meg. Miután a kliens azonosította magát a felhasználónév/jelszó párossal, létrejön a valós kapcsolat.

Ezzel szemben a titkosított hálózat a router által támogatott valamely biztonsági szabvánnyal védett hálózat. Ezek a szabványok erősségi sorrendben a következők: WEP, WPA és WPA2. Részletes beállítása a 2.4. fejezetben olvasható.

### 2.2.2.Tűzfal (firewall)

Manapság, amikor cégek, intézmények nagy számban csatlakoztatják hálózataikat az Internetre, a védelem egyik fontos eleme a tűzfal. A számítógépes hálózatokban a tűzfal egy olyan kiszolgáló számítógép vagy program, amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek, hogy az illetéktelen behatolásoknak ezzel elejét vegyék, egyúttal lehetővé teszi a kifelé irányuló forgalom ellenőrzését is. A tűzfal egyik típusa az úgynevezett „külső tűzfal” a teljes helyi hálózatot részben izolálja az Internettől, míg az úgynevezett „belső tűzfal” a helyi hálózat egy különösen védendő részét zárja el annak többi részétől, így az Internettől is. A tűzfal használata titkos, érzékeny adatok védelme, vagy nagy

üzembiztonságot kívánó hálózatok esetén elengedhetetlen. A tűzfal akkor alkalmazható hatékonyan, ha a teljes forgalom ezen keresztül zajlik le. A tűzfal nem a védelem alapeszköze, inkább fontos kiegészítője.

#### *2.2.2.1.Szabad zóna*

A tűzfalakat akkor tudjuk leghatékonyabban üzemeltetni, ha a belső és külső hálózat között helyezzük el őket. Sok esetben egy harmadik, a belső és külső hálózattól egyaránt eltérő hálózatra is szükség van, amit *szabad* vagy *demilitarizált* zónának neveznek. Ezt akkor használjuk, ha a nyilvános hálózatok számára elérhetővé akarunk tenni bizonyos kiszolgálókat pl. webkiszolgálót. Ennek az az előnye, hogy pontosan tudjuk szabályozni a zóna hálózati forgalmát. Ezzel a kalóztámadások egy részét is ki lehet védeni, mivel azok gyakran használják kiindulási pontként ezeket a kiszolgálókat, de ha azok külön hálózaton vannak, nem tudnak onnét betörni a védett belső hálózatra.

### 2.2.3. Jelszavak

Védelem szempontjából nagyon fontos szerepe van a jelszónak. Minél bonyolultabb és hosszabb jelszót választunk, annál nehezebb megfejteni. Vegyünk példaképp egy 40 karakteres jelszót. Ha ebből a 40 karakterből egyjegyű jelszót képezünk, 40 félét állíthatunk elő. Kétjegyű jelszó 40x40, vagyis $40^2$ lesz. Ha „n” jegyű a jelszó, akkor $40^n$ variáció lehetséges. Ha eggyel növeljük a jelszó hosszát, a lehetőség mindig 40-szeresére növekszik.

2. táblázat: A jelszóhossz növekedésével exponenciálisan nő a lehetséges jelszavak száma

| Jelszó hossza | Lehetséges jelszavak száma |
|---|---|
| 1 | 40 |
| 2 | 1 600 |
| 3 | 64 000 |
| 4 | 2 560 000 |
| 5 | 102 400 000 |
| 6 | 4 096 000 000 |
| 7 | 163 840 000 000 |
| 8 | 6 553 600 000 000 |
| 9 | 262 144 000 000 000 |
| 10 | 10 485 760 000 000 000 |
| 11 | 419 430 400 000 000 000 |
| 12 | 16 777 216 000 000 000 000 |

Alapszabályok, melyek betartása célszerű jelszavak megadásánál:

- minimum 10 karakter szükséges (már a WPA-nál is 20 karakter az ajánlott)
- könnyen megjegyezhető legyen
- gyakran cseréljük jelszavunkat, ne használjuk több helyen is ugyanazt!
- ne legyen benne olyan szó, ami a felhasználóra, vagy családtagjaira utal.

### 2.2.4. Hálózati titkosítás (Encryption)

A titkosítások leggyengébb pontja maga a kulcs, amellyel az adatokat kódoljuk, illetve dekódoljuk. Feladata kizárni a külső behatolásokat, kívülállóktól megvédeni az adatainkat. A titkosítás alapvető törvénye a *Kerckhoff-elv* szerint: a titkosítás biztonságát nem a kódolás során használt algoritmus erőssége, hanem a kulcs biztonsága határozza meg. A kulcs egy olyan adatsorozat, amellyel a kódolandó adatokat módosítjuk, a kódolásra jellemző algoritmus segítségével. Alapvetően kétféle titkosítás létezik: *szimmetrikus* és *aszimmetrikus*.

#### *2.2.4.1. Szimmetrikus titkosítás*

Az adatokat ugyanazzal a kulccsal dekódolhatjuk, amellyel titkosítottunk. A szimmetrikus titkosítás addig biztonságos, ameddig az adatokat csak a számítógép merevlemezén tároljuk, azokat nem küldjük el sehova. Előnye, hogy az általános szimmetrikus algoritmusok nagyon gyorsak, ha kevésbe komplikáltak, és a felhasznált kulcs mérete kisebb. Hátránya, hogy a korszerű adatátviteli módszereknek nem felel meg. Ha például a kódolt adatokat küldő fél az internetes kommunikáció során létrehoz egy kulcsot (ún. *session key-t*), akkor azt a kommunikáció összes résztvevőjéhez el kell juttatnia, különben a további kommunikáció megszakadna. Ha a támadó valamilyen módon el tudja fogni a kulcsot, akkor a további kommunikációt tudja dekódolni, és ez kiterjed a később frissített kulcsokra is.

#### *2.2.5.2. Aszimmetrikus titkosítás*

Az aszimmetrikus algoritmusok különböző kulcsokat használnak a kódoláshoz és a dekódoláshoz. Az aszimmetrikus kódolás két kulcsot használ. A küldő fél egy publikus kulccsal titkosítja az üzenetet, amelyet a fogadó korábban megosztott már a küldővel. Ezt publikus kulcsnak hívják, hiszen mindenki hozzáférhet, és a titkosítás ezzel a kulccsal csak zárható. A fogadó félnél van a privát kulcs, amelyet nem oszt meg senkivel, de dekódolni tudja a küldő által a publikus kulccsal kódolt adatokat. Mivel a privát kulcsot nem kell a kommunikáció során felhasználni, így az teljes biztonságban van. A publikus kulcsot viszont mindenkivel meg lehet osztani, hiszen működése egyirányú: az adatokat csak és kizárólag kódolni lehet vele. Ha a hacker elfogná a kódolt üzenetet és a publikus kulcsot, akkor sem tud mit kezdeni vele, hiszen nincs meg neki a dekódoláshoz használható kulcs. Hátránya azért ennek a módszernek is van, az adatok titkosítása mintegy ezerszer lassabb, mint a szimmetrikus algoritmusok esetén. A nagy számítási teljesítményt igénylő módszert ezért nagy mennyiségű adat titkosítására nem célszerű használni.

#### *2.2.5.3. Blokk és stream*

A kódolásokat egy másik, ugyancsak alapvető szempont alapján is kettéoszthatjuk: blokk vagy stream titkosításra. Az adatok *bitfolyamalapú (stream)* titkosítása valós idejű adatátvitel mellett használatos, például IP-telefonok levédésére. A kódolás már a kommunikáció elején elkezdődik, és a kódolt adatok azonnal útnak is indulhatnak a vevő felé anélkül, hogy blokkokat kellene létrehozni. A módszer előnye, hogy az így továbbított adatok

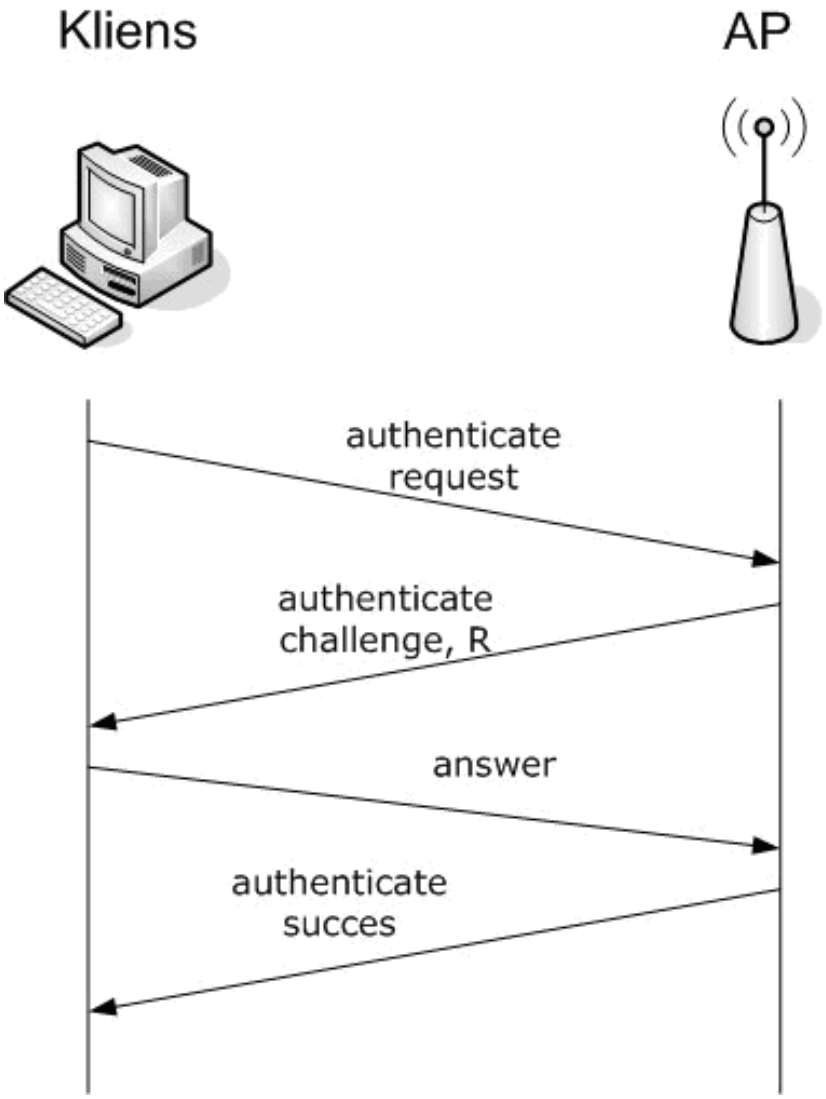
blokk hiányában kevésbé érzékenyek a kommunikáció hibáira, hiszen a hiba csak egy bitet érint, nem egy egész blokkot. A stream titkosítás hátránya viszont az, hogy összetett algoritmusok nem használhatók velük, a biztonság nagyságát ezért a hozzájuk tartozó szoftverkörnyezet határozza meg.

### 2.2.6. Hálózati hitelesítés (Authentication)

Azt biztosítja, hogy az informatikai rendszer felhasználói, folyamatai, erőforrásai és adatcsoportjai egyértelműen megkülönböztethetők legyenek, és az azonosítást valamely eszközzel ellenőrizni lehessen. Vagyis például kapcsolódhat-e az adott Wi-Fi hálózat AP-jához, és használhatja-e a vezeték nélküli hálózat erőforrásait, például az Internetet. Emellett létezik üzenethitelesítés is, amely már egy hitelesített viszonyban a titkosított üzeneteket védi a módosítással szemben (integritásvédelem). A WEP kétféle hitelesítési eljárást támogat: az egyik az úgynevezett *nyílt hitelesítés*, a másik az úgynevezett *osztott kulcsú hitelesítés*. Az előbbi esetben igazából nem is beszélhetünk hitelesítésről, csak igénybejelentésről, míg az utóbbi esetben a hitelesítő információ a közös WEP kulcs.

Általánosságban elmondható, hogy minden eszköznek a forgalmazás megkezdése előtt hitelesítenie kell magát az AP felé, mely egy négy lépcsőből álló üzenetváltásból áll (8. ábra):

1. A kliens (állomás) jelzi egy „authenticate request” küldéssel a hitelesítési szándékát az AP felé.
2. A hozzáférési pont egy véletlen számot generál és azt elküldi az állomásnak. Ez az „authenticate challenge”.
3. A kliens rejtjelezi ezt a számot a beállított WEP kulcsával és visszaküldi az eredményt az AP-nak „authenticate respond” („answer”) formában.
4. 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 az állomással „authenticate success” vagy hiba esetén „authenticate failure” formában.




8. ábra: A hitelesítés lépései

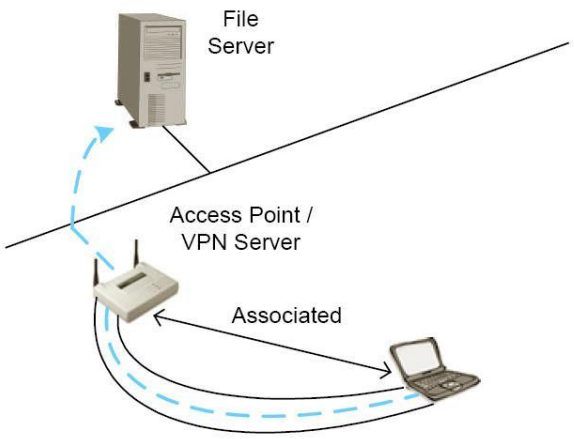
Ha a hitelesítés sikeresen végbemegy, akkor az adatforgalom titkosított formában történik, melynek kulcsa ugyanaz, mint amit a hitelesítéshez használnak, az algoritmus pedig az RC4 kulcsfolyam kódoló.

A titkosításnak és a hitelesítésnek együtt kell működnie, így garantálja a WLAN biztonságát!

## 2.2.7. VPN (Virtual Private Network)

Már 1990 óta használják vezetékes hálózatok interneten keresztüli titkos kommunikációjához. A WLAN-hoz is használható ez a kiegészítő védelem, segítségével két hálózatot kapcsolhatunk össze egy nem biztonságos hálózattal, vagyis az Internettel.

A felhasználónak rendszerint először egy kliensprogramot kell telepítenie, amelynek segítségével aztán a VPN szolgáltatást biztosító cég szerveréhez kapcsolódhat (9. ábra). Ezek után valamennyi, az Internetre küldött csomag ezen a szerveren keresztül jut ki a netre, a távoli számítógépek tehát a mi IP címünk helyett a szolgáltató szerverének címét látják majd. A mi gépünk és a szolgáltató közötti kommunikáció titkosított csatornán keresztül folyik, így az internetszolgáltató sem tud belehallgatni.




9. ábra: Virtuális magánhálózat

A VPN egyáltalán nem új megoldás, és nem is elsősorban a titkosításra szolgál, hanem arra, hogy a munkatársak biztonságosan hozzáférhessenek a cégek belső hálózatához is akár külföldi útjuk során is. A VPN lassabb, mint a közvetlen TCP/IP kommunikáció, ráadásul meg kell bíznunk benne. Ennek oka, hogy bár kívülről nem látszik, hogy pont mi mit csinálunk, maga a VPN szerver tudja, és így a szerver tulajdonosa is mindent tudhat rólunk. Ha egy hackernek sikerül feltörnie a szolgáltató gépeit, akkor megszerezheti nemcsak ezeket az adatokat, hanem a mi felhasználónevünket és jelszavunkat is.

## 2.2.8. WEP

Sokféle Wi-Fi - titkosítási metódus létezik, de fontos különbségek rejlenek közöttük. A WEP a legrégebbi módszer, de ha ezt használjuk, már akkor is jó úton járunk egy biztonságos hálózat kialakítása felé. Csakhogy a WEP könnyen feltörhető, ennek fő oka a hibás protokolltervezés volt. Az Interneten pillanatok alatt elérhetők olyan alkalmazások, amelyek segítségével minimális hozzáértéssel akár percek alatt bejuthat a támadó egy ilyen védett hálózatba. A haszna ennek ellenére megvan: sok támadó nem vesztegeti még ezt a kevés időt sem arra, hogy betörjön az ilyen hozzáférési pontokon keresztül, hanem keres egy könnyebb prédát. Komolyabb védelmet nyújt a WPA vagy utódja, a WPA2, amelyekben nagyrészt kiküszöbölték a WEP hiányosságait.

A WEP remek példája a stream titkosítás problémájának. A WEP protokoll a titkosított kommunikációhoz RC4 algoritmust használ, amelynek működése a következő: az RC4 először generál egy 0‑255 közötti véletlen számot (mindegyik 8 bites) a megadott kulcs alapján. Az így kapott adatokkal bitről bitre kódolja az elküldendő adatokat. A módszer egészen addig biztonságos, amíg a felhasznált kulcs elég hosszú, és azt csak egyszer használtak fel a hozzá tartozó véletlen számokkal együtt. A WEP protokoll azonban nem ragaszkodik a szigorú feltételekhez, hiszen amíg a kulcsot a router tárolja el (WEP key), az eseti kommunikációkhoz tartozó kulcsokat (session key, illetve *inititalization vector*) többször állítja elő. Ez eddig még rendben is lenne, de a WEP a 24 bites eseti kulcsokat minden adatcsomaghoz titkosítás nélkül hozzácsapja, és elküldi. A véletlenszerűen generált kulcsokból a 40 vagy 104 bites WEP kulcsot meg akkor is vissza lehet fejteni, ha viszonylag kevés kommunikációs adatot ismerünk. Márpedig a kulcsok általában 104 bit hosszúak, ha ehhez hozzáadjuk a 24 bites eseti kulcsot, akkor megkapjuk a köztudatban ismert 128 bites titkosítást. Kevesen tudják, hogy ebből máris 24 bit nyílt. Kezdetben használták még a 64 bites titkosítást (40 bit+24 bit eseti). A 152 és 256 bites titkosítás is elég ritka. Minden kulcsot hexa vagy karakteres formában adhatunk meg. 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. Ez az összefüggés a 3. táblázatban látható.

3. táblázat: A WEP kulcsok kialakításának logikája (Forrás: Takács – Rajnai, 2007)

| 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 | „abcdefghijklmnop” | „6162636465666768696a6b6c6d6e6f70” |
| 252 bit | 24 | 232 | 58 karakter | 29 karakter | „abcdefghijklmnopqrstuvwxyz123” | „6162636465666768696a6b6c6d6e6f70717273747576777879 7a313233” |

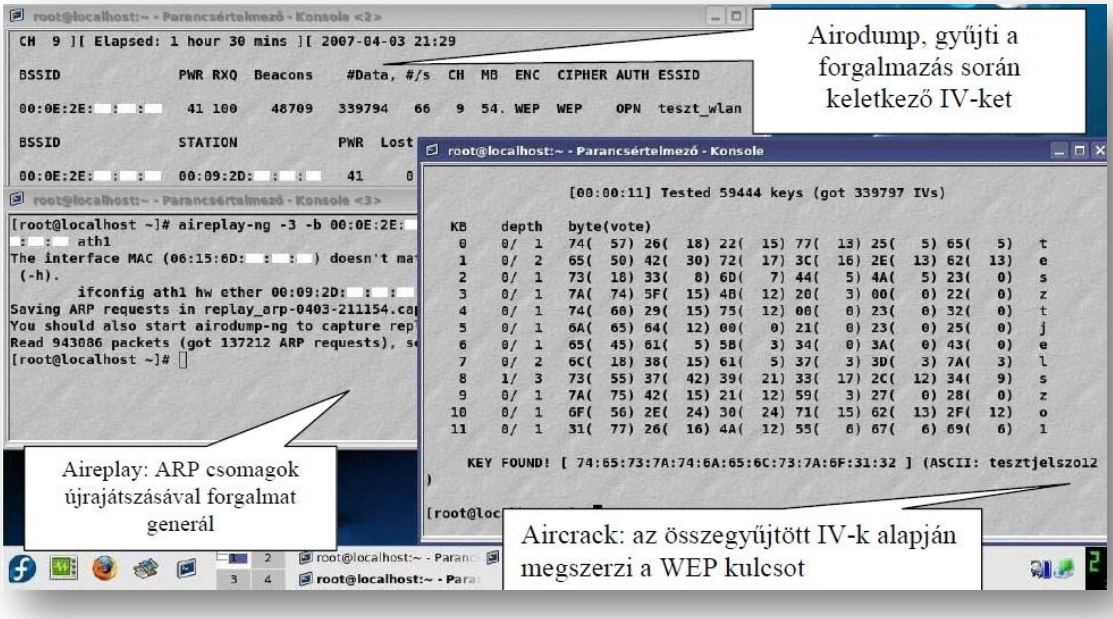
### *2.2.8.1. WEP hibái*

Legnagyobb hibája, hogy a hitelesítési kulcs, és a titkosítási kulcs megegyezik, így a támadónak elég az egyiket megszereznie. A *replay*, azaz a visszajátszásos támadásnál kihasználják, hogy a hitelesítés a hálózathoz csatlakozáskor csak egyszer történik meg. Ezután már bárki küldhet üzenetet az egyszer már hitelesített kliens nevében, annak MAC azonosítójával. 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. Mivel 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. A CRC védelem lenne hivatott kivédeni a replay támadásokat, ami a WEP-ből teljesen hiányzik. Másfelől csak a mobilállomás hitelesíti magát, így beleeshetünk egy olyan csapdába, hogy a saját hozzáférési pontunk helyett egy támadó által felállított, ugyanolyan nevű access pointra csatlakozunk. Ha ez megtörténik, akkor az adataink a betörőhöz érnek célba. A legnagyobb kiskapu maga a titkosítás, mivel az IV-k (inicializáció vektor) véges számúak, és ismétlődnek.

### *2.2.8.2. WEP feltörése*

Ahhoz, hogy sikeresen feltörjünk egy WEP titkosítású Wi-fi hálózatot, szükségünk lesz hozzá az Aircrack-ng szoftvercsomagra (10. ábra, forrás: Takács – Rajnai, 2007) és egy Linux operációs rendszerre. Ennek elég sok változata van, de feltöréshez a BackTrack a leghasznosabb disztribúció, mivel alapból sok beépített alkalmazást tartalmaz hálózatok

megfigyeléséhez. Az Aircrack-ng egy 5000 csomagból álló minta 40 bites kulcsát is percek alatt megtálalja, ehhez pedig elég egy átlagos teljesítményű számítógép.




10. ábra: Aircrack-ng Linux alatt

A támadás lépései:

- A wifi kártyát „promiscuous” (ún. „monitor”) üzemmódba kell kapcsolni. Adjuk meg „*airmon-ng start wifi0*” parancsot.

- Az Airodump-ng-vel feltérképezzük a közelünkben lévő eszközöket: „*airodump-ng ath1*”.

- Meg kell határoznunk célpontunk AP MAC címét és azt, hogy milyen csatornán dolgozik. Ehhez használjuk a Kismet nevű programot. Ha biztosra akarunk menni, szükségünk lehet egy hozzá csatlakozó kliens MAC címére is, mivel ezzel kijátszhatjuk azt, ha esetleg az AP-n be van állítva a MAC-cím szűrés. Ahhoz,hogy megszerezzük, a kliens hatósugarában kell lennünk.

- Indítsuk el az IV-k fogadását: „airodump --ivs --write adatok --channel 9 ath1”.

- IV-k számának növelése érdekében „érvényes” forgalmat kell generálni, mivel egy „kihalt”, csendes csatornán nem tudunk információkat begyűjteni. A forgalomgenerálás történhet „ARP request” csomagok elkapásával, azok visszajátszásával. Ezáltal felgyorsul a támadás, mivel minél több eseti kulcsot gyűjtünk be, annál gyorsabban megvan a jelszó. Ezt használja ki az Aircrack-ng program.

## 2.2.9. A 802.11i protokoll

Az IEEE által kidolgozott és jóváhagyott szabvány lényegében nem teljesen új átviteli protokollokat szabványosít, hanem meglévő, vezetékes környezetben korábban már széleskörűen alkalmazott eljárásokat implementál vezeték nélküli környezetbe. Tartalma igen szerteágazó, a vezeték nélküli hálózatokban eddig nem alkalmazott hitelesítési metódusokat és kriptográfiai újdonságokat foglal magában:

- IEEE 802.1x (vezetékes hálózatokban alkalmazott hitelesítési eljárások)
- EAP, RADIUS, WPA
- RSN (Robust Security Network)

Új kriptográfiai eljárások:

- CCMP (AES - CCM), TKIP (Temporal Key Integrity Protocol)
- Dinamikus kulcs csere és management

A fő hangsúly a hálózati hitelesítésen és annak biztonságán van, melynek modelljét a 802.1X szabványból kölcsönözték. Bár ezt a szabványt eredetileg vezetékes LAN környezethez tervezték, de WLAN-ban is alkalmazható. A 802.1X modell három résztvevőt különböztet meg a hitelesítés folyamatában: a hitelesítendő felet (supplicant), a hitelesítőt (authenticator), és a hitelesítő szervert (authentication server).

## 2.2.10. TKIP (Temporal Key Integrity Protocol)

A 802.11i egyik alappillérje. Tulajdonképpen egy kibővített változata a WEP-nek, mivel szintén RC4 kódolást használ, de a kulcs mérete már 128 bites. Amellett, hogy az alap kulcsot belekeveri a TKIP kulcsba, fontos változás a WEP-hez képest, hogy minden egyes adatcsomaghoz saját kulcs generálódik. A kulcs a küldő csomópont fizikai címéből és a csomag azonosítójából tevődik össze. Minden TKIP csomag el van látva egy 48 bites széria

számmal, mely eggyel növekszik, ha újabb csomagot küldünk. Az algoritmus ezt az értéket használja inicializációs vektorként és a kulcs részeként is. Ez a szekvencia szám biztosítja, hogy minden egyes csomaghoz külön kulcs tartozzon. Viszont közös osztott kulccsal való használatakor a hitelesítésnél használt 4-utas kézfogás titkosítatlansága miatt szótár alapú támadás hajtható végre a protokoll ellen.

### 2.2.11. AES (Advanced Encryption Standard)

Az AES a legújabb szimmetrikus titkosító szabvány. Alapja a *Rijndael algoritmus*, amely 128 bites blokkokat használ, és ezeket 128, 192 vagy 256 bites kulcsokkal titkosítja. A blokkokat a kulcs nagyságától függően 10, 12 vagy 14 lépcsőben újra és újra kódolják. A rendszer előnye a sebességre optimalizálás és az algoritmus könnyű implementálása szoftveres és hardveres megoldásokba. A 128 bites minimális kulcshossz garantálja, hogy az elkövetkező években *brute force* technikával se lehessen feltörni a vele védett adatokat. A 128 bit azt jelenti, hogy $2^{128}$ számú lehetséges kulccsal kell számolni, amely csak egy 39 jegyű számmal írható le. Ez még a ma használt szuperszámítógépeknek is sok ahhoz, hogy próbálgatásos módszerrel belátható időn belül feltörjék az AES-sel kódolt adatokat.

### 2.2.12. WPA, WPA2

A vezeték nélküli hálózatok biztonságát megalapozó 802.11i szabvány és a WPA2 tulajdonképpen ugyanazt fedi. Mindkét titkosítás a 802.11i-ből származik, ahol a WPA egy korábbi változat, és a WEP-pel ellentétben dinamikus kulcsot használ automatikus kiosztással, ráadásul erőteljes felhasználó-hitelesítést alkalmaz 802.1x és EAP használatával.

Az alapvető különbség a kettő között az alkalmazott titkosítási algoritmus: a WPA esetén *RC4/TKIP*, a WPA2 pedig egy továbbfejlesztett titkosító algoritmust használ, ez az *AES-CCMP*. A WPA2 jelenleg a legerősebb titkosítás, hátránya viszont, hogy csak a gyorsabb és drágább eszközök kiváltsága, mivel magas számítási kapacitást kíván meg az

eszközöktől. Előnye viszont, hogy visszafelé kompatibilis a WPA-val, így egy rendszerben egyszerre mindkét titkosítási módszer használható. Továbbá a vállalati felhasználásra szánt WPA2 változat autentikációs szervertől kapja a kulcsokat, ilyen például az AAA/RADIUS szerver.

2009-ben a technikai fejlődésnek köszönhetően feltörték a WPA közepes erősségű jelszavait az Elcomsoft Wireless Security Auditor programjával. Ez a program nemcsak a processzorokat, de a videokártyák GPU-ját is ki tudja használni, így csökkentve akár huszadára a feltöréshez szükséges időt. Ebből is látható, hogy a Moore-törvény szerint az RC4 alul fog maradni a versenyben. WPA2-nél még ez a veszély nem áll fenn, még mindig nincs meg a feltöréséhez szükséges technológiai háttér.

4. táblázat: Titkosítások összehasonlítása

| Titkosítás | Kódoló algoritmus | Kulcshossz | Inicializáló vektor |
|---|---|---|---|
| WEP | RC4 | 40 bit | 24 bit |
| WPA | RC4 | 128 bit: tikosítás<br>64 bit: hitelesítés | 48 bit |
| WPA2 | AES | 128 bit | 48 bit |

### 2.2.13. Titkosítás kvantumokkal

Egyelőre nem létezik olyan titkosító algoritmus, amely tökéletesen biztonságos lenne. A kvantumtitkosítás hívatott ezen változtatni. A hagyományos eljárások elsősorban a titkosító kulcs hosszától függenek – amelyet a nagy számítási teljesítményű számítógépek előbb-utóbb feltörnek. A kvantumtitkosítás biztonsága viszont a fizika törvényein alapszik. Már létezik olyan eljárás *(a BB84)*, amelyik fotonok állapotát (polarizációját) használja a bitek leképezésére, ily módon a titkosító kulcs átvitelére. A kommunikációt elfogni próbáló támadó nem tudja úgy lehallgatni az üzenetet, hogy ne változtatná meg azt (nincs klónozhatóság). Első lépésben megállapodnak a felek a kulcsban, amely random adatot tartalmaz. A küldő véletlenszerűen polarizált fotonokat küld a vevőnek. Ezzel együtt mindkét felhasználó

naplózza az adatokat, így mindkettejük számára meglesz a kulcs. A lehallgatás azért biztonságos, mert a lehallgató harmadik fél nem zavarja a kettejük közötti adást (ugyanazt a fotont lehallgatás közben nem tudja reprodukálni), illetve ha a lehallgató nem tudja megállapítani az üzenetküldés során használt kódot, akkor az általa mért bitek állapotáról sem tudja teljes biztonsággal megmondani, hogy 1-et vagy 0-t jelképeznek a kommunikáció során. A harmadik fél kommunikációba való lépését statisztikai módszerekkel ki lehet mutatni, így a csatornán átküldött adatok – legfőképpen pedig a kulcsok – biztonságosak maradhatnak.

## 2.3. Néhány támadási forma ismertetése

Két alapfogalmat érdemes tisztázni, amivel általában az emberek nincsenek tisztában, vagy egyszerűen csak összekeverik. Az Internetről idézem ezt a frappáns megfogalmazást: „a hacker a jóságos déli boszorkány, míg a cracker a gonosz nyugati. Vagy ha úgy jobban tetszik: ha valaki elmegy az OTP előtt, és látja, nyitva az ajtó, de nem megy be, csak beszól, hogy nyitva van, nos, akkor ő hacker. Ha viszont szó nélkül belép, és kihasználja a helyzetet, akkor az illető cracker.” A hacker önzetlenül segít feltárni és bemutatni a biztonsági réseket, míg a cracker egy bűnöző, aki anyagi haszonszerzés céljából teszi ezt. Újabban a hackereket megkülönböztetik feketekalapos, illetve fehérkalapos jelzőkkel.

### 2.3.1. Mérgezett hotspot

Nagyobb városokban szinte bárhol ütjük fel a noteszgépünket vagy okostelefonunkat, majdnem biztos, hogy találunk ingyenesnek tűnő, védelem nélküli Wi-Fi-hozzáférési pontokat. Újabban feltűntek úgynevezett „mérgezett” hotspotok. Vannak olyan támadók, akik nem emberbaráti szeretetből üzemeltetnek egy ilyen hotspotot, hanem azért, hogy a rácsatlakozott, gyanútlan gépek adatforgalmát elemezve megszerezzék adatainkat – legtöbbször azokat a hozzáféréseket, jelszavakat, amelyeket az ingyenes netkapcsolaton

keresztül használtunk. Óvakodjunk az ismeretlen hálózati azonosítóktól. Hacsak nincsen saját, biztonságos kapcsolási módunk (például VPN) mondjuk a munkahelyi hálózatra, akkor bármilyen nyilvános hálózaton netezzünk is, ne lépjünk be számunkra fontos, jelszót igénylő szolgáltatásba. Az ilyen helyeken híroldalakat vagy éppen az időjárást érdemes csak olvasgatni az interneten – ha igazán ügyelni szeretnénk a biztonságunkra.

### 2.3.2. Nyers erő támadás (Brute Force)

Számtalan ilyen, szótáralapú eljárás elvén működő, ingyenesen hozzáférhető jelszótörő program létezik. A program veszi az összes létező alfanumerikus karaktert, előállítja azok minden lehetséges kombinációját, titkosítja, majd összehasonlítja azt a megfejtendő jelszóval. Az eljárás vége a szerencsétől függ: befejeződhet gyorsan, vagy akár a végtelenségig is eltarthat. Ez a módszer hatékony, de nagyon időigényes és teljesítményfüggő is lehet. Minél hosszabb egy jelszó, annál több időt vesz igénybe a feltörése. Egy rövid jelszót már egy átlagos asztali számítógép is percek alatt megtalál. Újabban próbálkoznak azzal, hogy a processzornak besegít a számolásban akár több VGA-kártya is, ezáltal másodpercenként 22 ezer lehetséges jelszót lehet kipróbálni. Ez 15-ször gyorsabb működést jelent az eddigi hagyományos módszerekhez képest.

### 2.3.3. Plain Text

Olyan ez, mint egy kirakós játék. Logikája a következő: az éterben közlekedő hálózati küldemények, csomagok mindegyike tartalmaz egy kis részletet a kulcsból. Ha elegendő mozaikdarabkát sikerült összegyűjtenünk, már csak össze kell állítani, és teljes a kép. A hacker kiválaszt egy szövegrészt, és azt a titkosított szöveghez hasonlítva megpróbálja kitalálni a kulcsot. Ez persze csak akkor lehetséges, ha valamilyen módon meg tudja szerezni a titkosításhoz használt algoritmust, és egy titkosított adatrészt. A titok nyitja az a rész, amelyet a kódolt adatokhoz hasonlít. Ezzel a módszerrel adattárakat lehet hatékonyan feltörni. A hacker az archívum szabadon elérhető részeit kiválasztva keres a teljes, titkosított

archívumban. Ha nincs ismert rész, akkor is van esély a törésre: a titkosított e-mailek esetén a szokásos szófordulatok, címzés es üdvözlés szokott a kiválasztott rész lenni. Ezt a feltételezett részt kódolja be a támadó, majd összehasonlítja a titkosított résszel.

### 2.3.4. DoS (Denial of Service)

Szolgáltatásbénító támadásnak nevezzük az olyan támadási formákat, amelyek a közvetítő hálózatnak rontják le az áteresztőképességét, tönkreteszik az üzenetcsomagok áthaladását, vagy a hoszt számítógépeket terhelik le olyan szinten, hogy azok alig vagy egyáltalán nem lesznek képesek a hasznos hálózati kapcsolatok felépítésére. Ezt a támadó úgy éri el, hogy a hálózatban igen nagy adatforgalmat gerjeszt. A nagy terhelés megbéníthatja a hálózati kapcsolóeszközöket, de betelíthetik a közöttük lévő adatátviteli kapcsolatokat is. Ha a hacker a hoszt számítógépet veszi célba egy ilyen támadással, akkor olyan mennyiségű adatcsomagot, üzenetet küld, melynek feldolgozása annyira leterheli a számítógépet, hogy hasznos működésre képtelenné válik. Léteznek speciális üzenetek, melyek puffer túlcsordulást idéznek elő, a gép ennek következtében leáll. A támadás kivitelezésére tipikusan a hálózati protokoll hierarchia harmadik-negyedik szintjén lévő protokollokat (IP, ICMP, TCP, UDP) használják, melyeknek szabad átjárásuk van a hálózati kapcsolóelemeken. Ezen protokollok tervezésekor nem vették még figyelembe ezt a támadási lehetőséget, mivel az Internetet nem nyilvános hálózatnak szánták.

### 2.3.5. Rogue Access Point

Ezek az úgynevezett csaló hozzáférési pontok. A hackerek általában vállalati LAN hálózatokban szokták felállítani ezt az engedély és védelem nélküli hozzáférési pontot. Bárki, bármilyen nehézség nélkül hozzáférhet a cég adataihoz, akár az utcán is, ha erre az AP-re csatlakozik. Hozzá nem értés esetén akár felhasználó is létrehozhat ilyen hozzáférési pontot, ha nem veszi figyelembe a biztonsági előírásokat. Sok cég nem fordít különösebb költséget a megfelelő védelmi beállításokra, gyakran a router default beállításokkal működik.

Ennek kivédésére egyik lehetőség, ha a rendszergazda folyamatosan figyelemmel kíséri a hálózatot, vagy erőteljes hitelesítési módszert állítanak fel a rendszerben.

### 2.3.6. Közbeékelt támadás (Man-in-the-Middle)

Ez egyfajta kettős játék. A rosszindulatú behatoló megtöri a VPN-kapcsolat biztonságát, majd az elérési pont és a kliens közé állva a hacker képes elhitetni azt a klienssel, hogy ő egy access point. Ugyanígy becsapja a másik felet is, az elérési pontnak hitelesített kliensnek adja ki magát. Kezdetben passzívan figyel, összegyűjti a hitelesítéssel kapcsolatos információkat: az Access Point által küldött hívó *(challenge)* és összerendelési üzenet *(associate)*, a kliens azonosítóját, IP-címeket, stb. Ezek birtokában már nincsenek előtte akadályok.

### 2.3.7. Rejtett eszközök felderítése

Önmagában ma már nem segít, ha kapcsolódásunkat elrejtjük mások elől. Ilyen védekezés megkerülésére szolgál pl. a *redfang* vagy a *bluesniff* program. Segítségükkel felfedhető a rejtett eszköz gyártója és típusa, ezáltal a betolakodó új támadási stratégiát tervelhet ki. Telefonoknál az azonosítás a MAC-cím első 3 bájtja és az SDP rekordok lenyomata alapján történik.

### 2.3.8. Átirányítás rosszindulatú webhelyekre

Ez a módszer a biztonsági tanúsítványokat hamisítja, ha valaki belesétál a csapdába, akkor adatai máris a hacker szerverére kerülnek. Ilyen esetben, ha például beütjük a www.otp.hu webcímet, akkor böngészőprogramunk nem a bank, hanem a rosszindulatú rabló oldalára ugrik. A bejelentkezési oldalt pofonegyszerű imitálni és a felhasználó azt hiszi, hogy

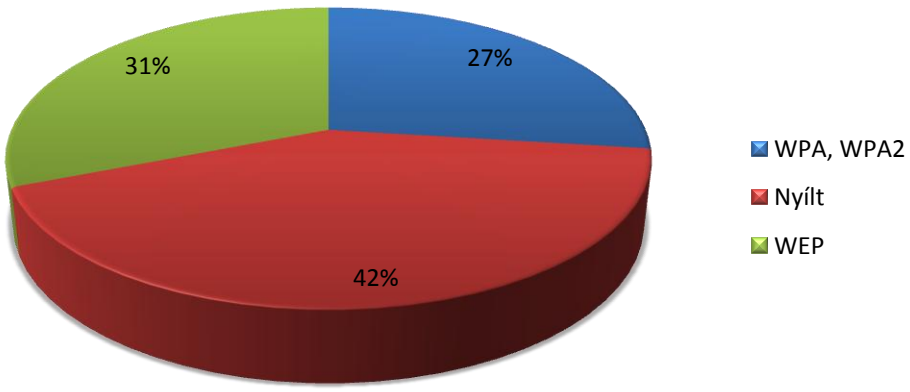
a bank rendszerében van (hiába jelzi a böngésző, hogy az oldal tanúsítványa nem jó, erre szinte mindenki „Tovább”- ot nyom, hiszen nem érti, mit akar a program), pedig csak annyi történt, hogy megadta egy ismeretlennek bankszámlájának legféltettebb kincsét: nevét és jelszavát.

## 2.4. Vezeték nélküli kapcsolatok védelmének biztosítása

### 2.4.1. Statisztika

Nagyobb városokban a hálózatok közel fele még mindig védelem nélkül áll. Ennek oka a következő: sok átlagfelhasználónak a WLAN routerek adminisztrációs menüje csak ritkán annyira felhasználóbarát, hogy megfelelően védje vele a hálózatát. Sokan csak a gyári beállításokkal működtetik eszközeiket. Az alábbi diagramon egy 2007-es budapesti felmérés eredménye látható (forrás: Takács – Rajnai, 2007):

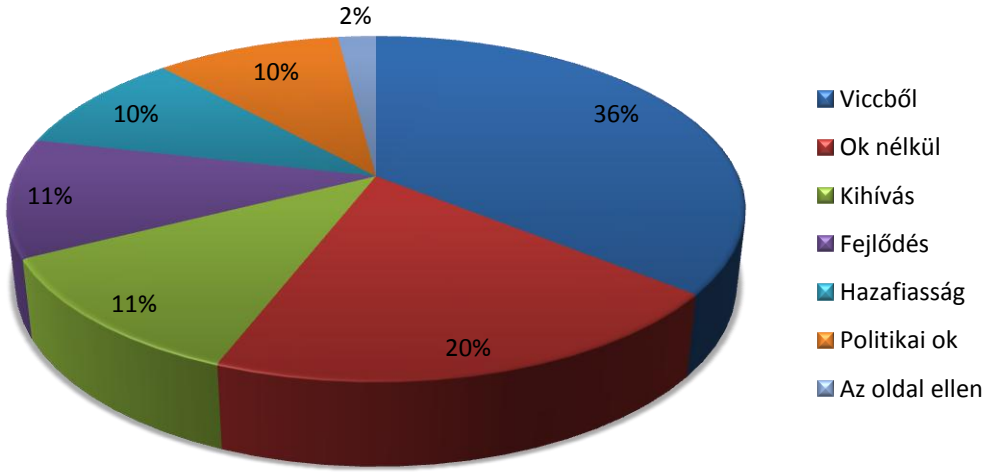
1. diagram: Titkosítások eloszlása




Sajnálatos módon a „győztes” a nyílt, védtelen hálózatok, melyekre gond nélkül felcsatlakozhat bárki. Második helyen még mindig az elavult WEP titkosítás áll. Bár

lehetséges, hogy valakinek kényszerből kell WEP-et használnia, mert régebbi kliense nem ismeri az újabb titkosítást. Mégis legutolsó helyen állnak a legjobb tudásúak: a WPA és WPA2.

2. diagram: Támadás okai




A második diagram a Zone-H internetes portál felmérése alapján készült. Sajnos a felmérés nem tért ki az anyagi haszonszerzés lehetőségére. Első helyen állnak a tréfák miatti elkövetések, második helyen az ok nélküli támadások, melyből következnek a harmadik helyen állók: a kihívás és a fejlődés.

Az eredmény annyira nem is meglepő, inkább az a kérdés, mi készteti rá az embereket számítógépek feltörésére. A szakirodalom megállapítása szerint a számítástechnikához értő, de visszahúzódó természetű emberek egy része ebben látja a kitörést; a megbecsülések megszerzésének egyik útját. Ezzel szerezhetnek elismertséget és hírnevet, melyek pozitív érzéseket keltenek az elkövetőkben.

## 2.4.2. A router beállítása

A fenti felmérés alapján úgy tűnik, az emberek nem igazán vesződnek még egy kezelési útmutató elolvasásával sem. Márpedig egy WLAN hálózatban a routerünk a kommunikációs központ, megfelelő biztonsági beállítása a legfontosabb.

A legtöbb esetben webes felületen végezhetőek el a beállítások. Ehhez kössük össze számítógépünket a routerrel, nyissunk egy böngészőablakot, és írjuk be a router IP-címét (például: 192.168.1.1). Ezt a címet úgy tudhatjuk meg, hogy a *Start* menü *Futtatás* sorában nyitunk egy DOS ablakot a *cmd* parancs kiadásával, majd kiadjuk az *ipconfig* parancsot. Itt az *Alapértelmezett átjáró* lesz a router címe. Ha nem kapnánk értelmes eredményt, akkor reseteljük a routert, és ellenőrizzük, hogy ad-e a számítógépünknek IP-címet. Ha tudjuk, hogy a router biztosan működik, de mégsem ad címet, gépünknek adjunk kézzel IP-címet (például 192.168.1.100), majd próbálkozzunk az 1-re végződő címmel, bár vannak olyan routerek, melyeknek IP-je 254-re végződik. Sikeres kapcsolódás esetén megjelenik a felhasználói nevünket és jelszavunkat kérő ablak. A felhasználói név általában „admin”, ritkán „root”, vagy üres. A jelszó „password”, „admin” vagy „default” szokott lenni, de ez is lehet üres. Első dolgunk az legyen, hogy választunk egy új jelszót magunknak, különben előfordulhat, hogy csak resetelés után tudunk belépni a router menüjébe, mert valaki „kitalálta” és megváltoztatta a jelszót. A jelszavakat leggyakrabban a *Settings*, *Advanced Settings,* illetve *System* alatt lévő *Administration,* és *Router password* opcióknál adhatjuk meg.

Ha a gyári jelszó cseréjén túl vagyunk, akkor válasszunk magunknak titkosítást. A WLAN titkosítását a következő módszerekkel védhetjük: WEP (Wired Equivalent Privacy), WPA-PSK (WiFi Protected Access – PreShared Key) és WPA2-AES (WiFi Protected Access – Advanced Encryption Standard). Létezik WPA2-PSK és WPA2-AES+TKIP (Temporal Key Integrity Protocol) is, ráadásul még ezeknél is biztonságosabb, hitelesítő szervert igénylő rendszer is (például a Radius). Engedélyezzük a WLAN kommunikációt a *Wireless Settings* alatti *Enable Wireless Network (WLAN)* opció bejelölésével. Sok esetben csak akkor lesz aktív a kapcsolat, ha a beállítások elmentése után újra is indítjuk a routert, ezt az adminisztrációs vagy rendszer menüben, *Restart router* vagy *Reboot router* gombbal tehetjük meg. A titkosításnál az összes készülék elérhető legjobb biztonsági rendszerével érjük el a legjobb hatást. Régi kliensekhez általában elérhető újabb szoftver is, azt telepítve már a WPA-

t is használhatjuk. Ha még sincs hozzá frissítés, akkor jobb híján állítsunk be WEP-et 128 bites kulccsal. Fontos, hogy ezek az adatok – a jelszavakat is beleértve – minden készüléken azonos módon legyenek beállítva. A jelszavak és kódok minimum 10 karakter hosszúak legyenek, nagybetűket és számokat is tartalmazzanak. Ha mindezekkel kész vagyunk, válasszuk ki operációs rendszerünkön a saját hálózatunkat, és írjuk be a jelszavunkat (ezt általában csak egyszer kell megadnunk).

Nem ritka, hogy a biztonságos hálózat sebessége látványosan csökken – ekkor érdemes csatornát váltani, mert valószínű, hogy a környező WLAN routerek éppen a miénket használják. Lehetőség szerint az 1-es, 6-os, 12-es közül válasszunk, minél messzebb a többitől. Ezt szintén a router menüjében állíthatjuk be. A WEP- vagy WPA-titkosítás engedélyezése csökkentheti az adattovábbítás sebességét, fontos tehát, hogy a kiinduló jel erős legyen. Ne essünk abba a hibába, hogy a teljesítmény fokozása érdekében kikapcsoljuk a titkosítást. Továbbá, ha előre tudjuk, kik csatlakoznak a hálózatunkhoz, akkor kapcsoljuk ki a DHCP-t vagy megváltoztathatjuk routerünk gyári IP címét is.

## 2.4.3.További védelmi vonalak felállítása

### *2.4.3.1. Az Access Point körültekintő elhelyezése*

Érdemesebb a lakás középpontjában elhelyezni, vagy a szórást a lakás méreteihez igazítani, mivel ablak vagy fal közelében a rádióhullámok könnyen kijutnak. Tiltsuk le az ad-hoc módot, különben a kliensek bármelyik más klienshez csatlakozhatnak az access point nélkül is.

### *2.4.3.2. Forgalommonitorozás*

Használjuk a beépített lehetőségeket forgalommonitorozásra, mint például a *rogue detection* lehetőséget, mely figyeli a betolakodókat. Másik alternatíva a *traffic delivery*, mely figyelő-, és adatszűrő rendszerként funkcionál. Ezek a beállítások minimálisan terhelik le a rendszerünket, mégis sokat segítenek a támadók időbeni észlelésében.

#### *2.4.3.3 MAC-szűrés*

Alacsonyabb szinten véd a MAC (Media Access Control) címeket felügyelő rendszer, amely a legtöbb routeren *MAC Filter* névre hallgat. Ha engedélyezzük, akkor a router csak azokat az előre megadott listán szereplő eszközöket hajlandó kiszolgálni, amelyek egyedi (gyártás során kapott) MAC-címükkel azonosítják magukat. Mivel a MAC-cím lehallgatható az éterben, csak program kérdése, hogy a támadó a gépét az engedélyezett címek egyikére írja át. Ilyen program ma már Windowsra is létezik, sőt, a registry-ben is megváltoztatható egy hálózati kártya MAC-címe.

#### *2.4.3.4. SSID (Service Set Identifier)*

Olyan, maximum 32 karakterből álló egyedi azonosító, amely minden egyes vezeték nélküli hálózaton küldött csomag fejlécében szerepel. Érdemes megváltoztatnunk, mivel alapértelmezettként routerünk típusát mutatja másoknak, ez pedig könnyíti a behatolási lehetőséget.

Érdekes az SSID-éknél az a fajta pszichológiai hadviselés, hogy minél elrettentőbb nevet adnak a felhasználók otthoni hálózatuknak. Megemlítenék pár finomabb közlést, mint pl.: gyilkos, tűnj el, ne lopj, stb. Furcsa eltántorítási módszer, de egy vérbeli rosszindulatú hacker azonnal kíváncsi lesz, mit rejthet egy ilyen számítógép.

#### *2.4.3.5. Firmware*

Ha routerünkhöz újabb gyári firmware érhető el, amely tulajdonképpen az eszköz belső szoftverfrissítése, akkor azt telepítve nagyobb biztonsághoz, illetve sebességhez juthatunk. A frissítést szigorúan csak LAN oldalról végezzük el! Ha vezeték nélkül próbálkozunk és megszakad a kommunikáció, a routerbe írt adatok is hibásak lesznek, ennek eredménye pedig egy használhatatlan router lesz.

# 3. Összegzés

A vezeték nélküli hálózatok mára széleskörűen elterjedtek otthonainkban is, hiszen ezek segítségével könnyen megosztható az internetelérés több számítógép között, ráadásul fejlődésükben az elkövetkezendő években további exponenciális növekedés várható. Telepítésük kis költséggel jár, fenntartásuk sem drága, így a kezdeti befektetés hamar megtérül. Már ma is megvan a lehetőségünk hozzá, hogy teljes értékű WLAN-hálózatokat építsünk ki nagyon rövid időn belül például egy konferenciát szervező szállodában, egyetemi campusban vagy akár a szabad ég alatt. Az internet-hozzáférés mindennapossá válása további igényt hozott a felszínre: megjelentek a forgalmasabb tereket, épületeket, repülőtereket, éttermeket lefedő nyilvános WLAN-rendszerek, melyek elsődleges feladata a világhálóhoz való hozzáférés nyújtása az emberek számára. Természetesen ezzel együtt fokozottan jelentkeznek a hozzáférési jogosultság kérdései.

Ami áldás a kényelem szempontjából, az bizony rémálom lehet biztonsági oldalról. Minden hálózat tulajdonosának mérlegelnie kell, hogy mennyit ér meg az adatai biztonsága. Sajnos a védekezés szükségességére sokan csak akkor jönnek rá, amikor megtörtént a baj és az adatok illetéktelen kezébe kerültek, vagy ha a hatékonynak vélt szoftveres védelem megbukott. Az olyan apró mulasztások, mint a rosszul beállított tűzfal, a frissítetlen Antivirus szoftver vagy a hiányzó biztonsági javítások illetéktelenek számára hozzáférhetővé tehetik adatainkat, vagy akár a mi gépünket használva kéretlen reklámlevelet küldhet, másokat zaklathat, betörhet különböző kiszolgálókra, így a betörés nyomai hozzánk vezetnek, a betörő pedig névtelen maradhat. Tehát minden biztonsági óvintézkedés ellenére azonban ne feledjük: ha vezeték nélküli rendszert használunk, mindig legyünk tudatában annak, hogy sokkal sebezhetőbbek vagyunk.

Dolgozatom célja a legismertebb vezeték nélküli hálózatok bemutatása és az ezekkel kapcsolatos legfontosabb biztonsági kérdések ismertetése. Megismerhetjük a Wi-Fi kialakulását, fejlődési stádiumait, kiterjedéseik közötti különbségeket. Részletesen kifejtettem a WEP és WPA titkosítási és hitelesítési folyamatait, valamint a jövő titkosítási lehetőségét, amely a kvantumokra épül. A statisztikai felmérésben diagramokon ábrázoltam a felhasználók

által használt titkosítások eloszlását, és a támadások okait. Továbbá olvashatunk az egyes feltörési módszerekről; a megelőzésükről pedig részletes router beállításokkal zártam dolgozatomat. Konklúzióm a témával kapcsolatban, hogy a felhasználók figyelmetlensége, és könnyelműsége miatt történhet a legtöbb feltörés. Bármilyen titkosítást is alkalmazunk, a legbiztonságosabb rendszer még a mai napig is egy kikapcsolt számítógép.

# Irodalomjegyzék


1. **[CHRIS HEEGARD]**

Chris Heegard, John (Seán) T. Coffey, Srikanth Gummadi, Peter A. Murphy: High-Performance Wireless Ethernet, 2001.

2. **[AJAY CHANDRA V. GUMMALLA]**

Ajay Chandra V. Gummalla and John O. Limb: Wireless Medium Access Control Protocols, 2000.

3. **[WIKIPEDIA]**

WLAN: http://en.wikipedia.org/wiki/Wireless_LAN

BB84: http://en.wikipedia.org/wiki/BB84

4. **[CHRIS HURLEY]**

Chris Hurley: WarDriving & Wireless Penetration Testing, 2006.

5. **[INTEL]**

Barneo: http://www.intel.com/cd/corporate/pressroom/emea/hun/212658.htm

6. **[LINUXVILÁG]**

Hálózat építése:http://www.linuxvilag.hu/content/files/cikk/77/cikk_77_66_68.pdf
Adatvédelem: http://www.linuxvilag.hu/content/files/cikk/73/cikk_73_11_14.pdf

7. **[BUTTYÁN LEVENTE]**

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

8. **[OROSZ PÉTER]**

Orosz Péter, Gál Zoltán, Karsai Andrea – Adatbiztonság elemzése mobil WiFi környezetben, Debreceni Egyetem Informatikai Központ.

9. **[FAIGL LÁSZLÓ]**

Faigl László: Az IEEE 802.11i kapcsolat-felépítés vizsgálata – RADIUS alapú hitelesítés EAP-TLS módszerrel WLAN hálózatban, 2005.

10. **[IHM-MTA]**

IHM-MTA Sztaki: Az informatikai hálózati infrastruktúra biztonság kockázatai és kontrolljai, 2004.

11. **[KRASZNAY CSABA]**

Krasznay Csaba: Vezetéknélküli hálózatok (WiFi, Bluetooth) biztonsága, Kancellár.hu Kft. Weboldal: http://www.krasznay.hu/prez_hu.html

12. **[PC WORLD]**

http://pcworld.hu/80211-draft-n-routerek-tesztje-20080501.html?p=4

Magazin: 2008. évfolyam, júniusi szám.
2008. évfolyam, augusztusi szám.
2009. évfolyam, szeptemberi szám.
2010. évfolyam, márciusi szám.

13. **[WHITEPAPER]**

http://ce.computers.toshiba-europe.com/Contents/Toshiba_ce/CE-HU/WHITEPAPER/files/2006-09-WWAN-for-business-CE.pdf

14. **[TAKÁCS PÉTER]**

Takács Péter – Rajnai Zoltán: A WiFi hálózatok veszélyei, II. Évfolyam 2. szám - 2007. június.

15. **[F. Ható Katalin]**

F. Ható Katalin – Adatbiztonság, adatvédelem, Számalk kiadó, Budapest, 2000

16. **[WYONAIR]**

http://www.wyonair.com/wifi-wlan_mi_a_wlan.php

http://www.wyonair.com/wifi-wlan_biztonsag.php

17. **[BME]**

http://alpha.tmit.bme.hu/meresek/lanfiz.htm

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

18. **[CHIP]**

Magazin: 2009. évfolyam, februári szám.
2009. évfolyam, novemberi szám.

19. **[EGYÉB KÜLFÖLDI FORRÁSOK]**

http://www.wi-fi.org/knowledge_center/kc-howandwhyofwi-fi

http://www.pulsewan.com/data101/802_11_b_basics.htm

http://compnetworking.about.com/cs/wireless80211

20. **[EGYÉB MAGYAR FORRÁSOK]**

http://index.hu/tech/cellanaplo/2009/12/29/feltortek_a_mobilhalozatok_titkositasat/

http://www.hiradastechnika.hu/data/upload/file/2005/2005_8/HT_0508-2.pdf

http://www.hoc.hu/teszt/402-tp-link-draft-n-es-eszkozok-tesztje/2-egy-kis-elmelet.html

http://itcafe.hu/cikk/vedtelen_wi-fi_halozatok/nyomtatobarat/teljes.html

http://www.scribd.com/doc/28204223/WLAN-vezeteknelkuli-LAN

http://biztonsagportal.hu/wi-fi-betolakodo-elharitas.html

http://www.bcs.hu/index.php?akt_menu=494#top

http://miau.gau.hu/mediawiki/index.php/WLAN

# Függelék

**Törvény:**

Az EU-tagságunkat és sok másik ország törvényhozását is megelőzve nálunk igen hamar életbe lépett a BTK. 2001 évi CXXI. törvénye – a rosszindulatú hackerek ez alapján büntethetők. A 2001 óta érvényes törvény 300/C § szerint: „aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad, vétséget követ el, és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.” Tehát a jelszavak visszafejtése vagy kiiktatása után – hacsak az nem a saját rendszerünk – még belépni is tilos.

# Köszönetnyilvánítás

Ezúton szeretném megköszönni témavezetőm, Dr. Krausz Tamás segítségét, hogy tanácsaival, javaslataival hozzájárult szakdolgozatom elkészítéséhez, valamint a szükséges segédanyagokat rendelkezésemre bocsátotta.