ÓBUDAI EGYETEM
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

Szakdolgozat

Vezeték nélküli hálózatok támadóinak lokalizálása

Készítőjének neve: **Csaba Tamás Gábor**
Neptun kódja: RNS4WG

Budapest
2013

Tartalomjegyzék

BEVEZETÉS

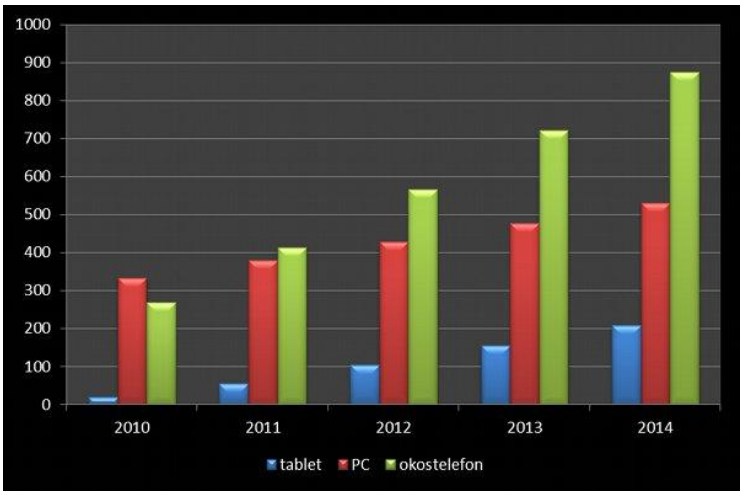
A vezeték nélküli hálózatokat számos helyen nem használják az emberek bizalmatlanságukban, például minősített adatok, vagy céges titkok továbbításra, mivel az ilyen adatokat nem szívesen bízza rá az ember rádióhullámokra, amik vagy célba érnek, vagy nem, és vagy lehallgatják őket vagy nem. Ma már több megoldás is van ezek kiküszöbölésére, az adatokat titkosítása, a számítógépek hitelesítése, a hálózat elrejtése vagy egyéb módok, amelyek lehetővé teszik hálózat védelmét az illetéktelenektől. Azonban mint tudjuk, a támadók mindig egy lépéssel előttünk járnak, és kitalálnak valamit a védelem áttörésére, vagy megkerülésére, így a fontos adatokat továbbra is inkább vezetékes úton továbbítják. A nyári gyakorlatomat a Magyar Honvédség Veszélyesanyag Ellátó Központnál töltöttem el, ahol többek között a Híradó és Informatikai főnökségen is voltam, az ott dolgozók el mondták, hogy náluk teljesen tiltott ez a technológia, és az egész számítógépes hálózatuk vezetékes, ők többek között így védik az adatokat.

Mint tudjuk az információ hatalom, így az informatikai védelem a komplex vagyonvédelem 4. ága lehet, hiszen ha egy céget veszünk, aminek nincs vezeték nélküli hálózata, akkor az információt elsősorban a fizikai védelem, az elektronikai jelzőrendszer, és az élőerős védelem védelmezi. Abban az esetben, ha a támadó átjut ezeken, és egy kapcsolódási ponthoz hozzáfér, gyakorlatilag bármilyen adathoz hozzáfér, és ha még észre is veszik, hogy épp adatlopás történik, az egész épületet, vagy telephelyet át kell kutatni, hogy megtalálják az illetőt.

Ha a komplex vagyonvédelem eszközei mégis képesek megvédeni a hálózatot, akkor gyakorlatilag külső személy nem férhet hozzá, és sokkal biztonságosabb, mint a vezeték nélküli társa, én még is úgy gondolom, hogy a vezeték nélküli technológiáé a jövő, jól megfigyelhető már napjainkban is. Egyre több irodai eszköz tud már csatlakozni ilyen hálózathoz, a munkaállomások egyre kisebbek, ma még PC-ken, vagy Laptopokon dolgozunk, de ki tudja, pár év, és Tableteket, és okostelefonokat fogunk erre használni, amik méreteikből adódóan sincs lehetőség egy UTP kábel csatlakoztatására. Az embernek is kényelmesebb, ha az irodájában felállhat, sétálhat, és közben egy ilyen eszközön „pötyög”, és nem röghöz kötve egy PC előtt görnyed.

Az 1. diagram a Gartner nevű elemző cég által összegyűjtött, és becsült eladási adatai láthatóak, jól kivehető, hogy a vezeték nélküli kommunikációra alkalmas Tabletek, és

Okostelefonok eladási adatai kimagaslóan emelkednek. A függőleges tengelyen az adatok millió darabként értelmezendők. [1]



1. Diagram: Előre jelzett eladási adatok

Forrás: [1]

Ma már képesek vagyunk a gondolatainkkal irányítani gépeket, vagy hologramokat vetíteni, amiket megérintve interakciót kezdeményezhetünk, és mindezt bele bírjuk zsúfolni néhány pici eszközbe. Ezek fényében úgy gondolom, a vezeték nélküli hálózatoké a jövő.

A szakdolgozatom elkészítésénél célul tűztem ki magam elé, hogy ismertessem a vezeték nélküli hálózatok eszközeit, az ide vonatkozó szabványokat, a vezeték nélküli hálózatok védelmének a módjait, azokat a támadási formákat, amikkel támadhatók ezek a hálózatok, ismertetni a rádióhullámokkal kommunikáló eszközök helymeghatározásának módszereit, és egy olyan módszer megtervezése, és kidolgozása, amellyel felderíthetőek a hálózat támadói.

Ezt a célt már csak azért is érdemes szem előtt tartani, mivel mindenki tudja, hogy feltörhetetlen, vagy megkerülhetetlen védelem nem létezik, vagyis még a legkomolyabb védelemmel rendelkező hálózat is feltörhető a megfelelő eszközkészlettel. Megfelelő rendszergazdai felügyelettel előfordulhat, hogy célszerűbb a támadót nem kizárni a hálózati forgalomból, hanem a kommunikációt egy biztonságos térbe terelni, ahol a támadó nem tud kárt okozni, eközben a beavatkozó erők, a rendszergazda segítségével megkeresik a támadót, rákényszerítik tevékenysége felfüggesztésére, és visszatartják a rendőrség kiérkezéséig.

1. FEJEZET: VEZETÉK NÉLKÜLI HÁLÓZATOK SZABVÁNYAI

1.1 Vezeték nélküli hálózatok kialakulása

A Wi-Fi-ként ismert hálózatok alig néhány évtizedes múlttal rendelkeznek, de a gyökerei már az 1940-es évekre visszavezethetőek.

1942-ben George Antheil zeneszerző és zongoraművész és Hedy Lamarr színésznő szabadalmaztatták a frekvenciaugrásos rádiótitkosító eljárást, amit Spread Spectrum Modulation[1] neveztek el.

1958-ban az amerikai haditengerészet kifejlesztett egy a szórt spektrumú moduláción alapuló rádió kommunikációs chipet.

1985-ben a civil szféra számára is elérhetővé tették a korábban csak a katonaság által használhatott technológiát, de csak 1989-ben engedélyezte az FCC[2] a technológia alkalmazását 3 szabad rádiósávra.

Az első vezeték nélküli hálózatok megjelenése koránt sem volt problémamentes, ahogy azt már megszokta az emberiség egy új technológia megjelenésénél. Számos probléma merült fel, az első változatokkal, az alacsony sávszélességtől kezdve, a biztonsági kérdésekig. Arról nem is beszélve, hogy szabványok híján minden gyártó úgy alakította ki az eszközeit, ahogy tudta, így azok az eszközök csak olyan más eszközökkel voltak teljesen kompatibilisek, amelyiket ugyan az a gyártó gyártott.

1991-ben több gyártó közreműködésével létrejött a WECA[3] a problémák kiküszöbölésére. A szervezet később Wi-Fi névre neveztette át magát, és célja a vezeték nélküli technológiák szabványosítása volt.

1997-ben az IEEE[4] kiadta a 802.11-es szabványcsaládot, amely a vezeték nélküli hálózatokat definiálta.

A 802.11-es szabványcsalád megjelenésével elkezdődhetett a technológia elterjedése, hiszen a gyártók megkaptak bizonyos sarokköveket, amiket így már nem kellett kifejleszteniük, a fejlesztési idő lecsökkent, a költségek csökkentek, az eszközök megbízhatósága pedig nőt. Ezek után a vezeték nélküli hálózatok rohamosan terjedtek.

---

[1] Spread Spectrum Modulation: Szórt Spektrumú Modulációnak
[2] FCC: Federal Communications Commission – Amerikai Hírközlési Hatóság
[3] WECA: Wireless Ethernet Compatibility Alliance
[4] IEEE: Institute of Electrical and Electronics Engineers

2000-től egyre többen indítottak WLAN szolgáltatásokat, és egyre több eszköz jelent meg, amelyekkel ezek a szolgáltatások igénybe vehetőek voltak.
2005-re fél milliárdra jósolták a WLAN-t támogató eszközök eladását. [2 pp. 6-7]

1.2 IEEE szabványcsalád

Az IEEE szabványcsalád mára 6 szabványból áll, a 802.11, 802.11a, 802.11b, 802.11g, 802.11n, és a legújabb 802.11ac szabványból. A szabványok az adatátvitel legalapvetőbb kérdéseivel foglalkoznak, az adatátviteli sebességgel (egységnyi idő alatt átvitt adat mennyisége), távolsággal (a rádióhullámok milyen messzire terjedjenek), a rádióhullámok frekvencia tartományával, és a fellépő interferenciák (a rádióhullámokat gyengítik a tereptárgyak, amikbe ütköznek, de más készülékek rádió sugárzása is zavarhatja a jelet) kezelésében.

1.2.1 IEEE 802.11 szabvány

A 802.11-es szabvány volt az első IEEE által kiadott szabvány. A szabvány 1997-ben jelent meg. Az adatátviteli sebesség maximum 1-2 Mbit/sec lehetett, az adatátvitel módja pedig az infravörös fény, és a 2,4 GHz-es frekvenciatartományú rádióhullámok szerepelnek. Rádióhullámok esetén az FHSS[5] vagy a DSSS[6] eljárás használható. A szabvány definiálta a közeghozzáférést szabályozó CSMA/CA eljárást is.
A szabványt, megjelenésével több gyártó is felhasználta a termékeiben, ám igen sok teljesítményi, együttműködési és biztonsági probléma merült fel, amik kezdetben igen sok fejtörést okoztak a mérnököknek.
Az elméleti hatótávolság beltéren körülbelül 20 m, kültéren körülbelül 100 m. [2 p. 21] [3]

1.2.2 IEEE 802.11b szabvány

Bár az ABC-ben az „a” következne, és már korábban utaltam rá, hogy van 802.11a szabvány is, időrendben a 802.11-es szabványt a 802.11b jelű szabvány követi, ami az első kiegészítése az eredeti szabványnak. A 802.11b szabvány 1999-ben jelent meg, amelyet 802.11 High Rate-nek is neveznek, mivel a fizikai réteg nagy sebességű kiegészítését tartalmazza DSSS rendszerekhez.

[5] FHSS: Frequency Hopping Spread Spectrum – Frekvenciaugrásos Szórt Spektrum
[6] DSSS: Direct Sequence Spread Spectrum - Direkt Sorozatú Kiterjesztett Spektrum

A szabvány a 2,4 GHz-es frekvenciatartományt használja, az adat adatátvitel sebességét pedig 11 Mbit/sec-ra növeli, az eredeti többszörösére. Ez a sebesség már jóval gyorsabb, mint az DSL, így alkalmas otthoni internet megosztásra.
A 11 Mbit/sec sajnos csak elméleti sebesség, a gyakorlatban ez körülbelül 4-6 Mbit/sec-ot jelent.
A 802.11b szabványra épülő hálózatok tipikusan a pont-multipont felépítésben használják, vagyis egy AP-hoz több eszköz csatlakozhat.
Az ilyen hálózatoknál az AP általában egy körsugárzót használ, amely a tér minden irányába sugározza a rádióhullámokat. Az ilyen kiépítés elméleti hatótávolsága körülbelül 38 m beltéren, és körülbelül 140 m kültéren.
Pont-pont összeköttetés esetén jóval nagyobb hatótávolságok is áthidalhatóak (km-es nagyságrendek) irányított antennák segítségével.
Nagy előnye a 802.11b szabványt használó eszközöknek, hogy nagyon elterjedtek, és nagyon olcsóak is, ezért rengeteg elektronikai eszközünkbe építik be napjainkban is, pl. okostelefonokba, PDA-kba.
Hátránya, hogy napjainkra a 2.4 GHz-es frekvenciatartomány elégé telített, rengeteg az ebben a tartományban működő eszköz, ami igen komoly interferenciákat okozhat, komoly sebességvesztést, vagy a kapcsolat megszakadását okozhatja.
A 802.11b kompatibilis visszafelé a 802.11 szabvánnyal, egyszerűen leszabályozza az adatátviteli sebességet. [2 pp. 21-23] [3]

1.2.3 IEEE 802.11a szabvány

Ugyancsak 1999-ben jelent meg a 802.11-es szabvány második kiegészítése, a 802.11a jelű szabvány. Ez a szabvány szinte egyszerre jelent meg a 802.11b-vel, és bár vannak hasonlóságok a szabványok között, de rengeteg mindenben különböznek. A legnagyobb változás, az 5GHz-es frekvenciatartomány használata, ami számos előnnyel jár. Az 5GHz-es frekvenciatartomány még alig használt, kevés az interferenciát okozó eszköz, és a nagyobb frekvenciatartomány nagyobb sávszélességet is eredményez. Az 5 GHz-nek köszönhetően a sávszélesség 54 Mbit/sec elméleti sebességre nőt, ami a gyakorlatban 21-22 Mbit/sec. Az 5GHz-es tartomány nagy hátránya, hogy a hatótávolság csökken a 802.11b szabványhoz képest, és hogy ez a jel könnyen elakad a különböző tereptárgyakban.
Az elméleti hatótávolság beltéren körülbelül 35 m, kültéren 120 m, ami a gyakorlatban azért sokkal kevesebb.

Ezt ellensúlyozandó a 802.11a szabvány több egymást át nem fedő „csatornát” használ, amelyet akár egyszerre is igénybe vehetünk, ami lehetővé teszi, hogy a felhasználók akkor se érezzenek jelentős sebességcsökkenést, ha éppen komoly adatforgalmat bonyolítanak a hálózaton (nagy méretű fájlokat másolnak, filmet néznek). Ezt az OFDM[7] kódolási technológia teszi lehetővé.

Komoly probléma a 802.11a szabvánnyal, hogy nem kompatibilis önmagában se a 802.11, se a 802.11b szabvánnyal, az eltérő frekvenciatartomány miatt. Külön bővítő modul szükséges a kapcsolat létrehozásához. [2 pp. 23-24] [3]

1.2.4 IEEE 802.11g szabvány

A 802.11g szabványt 2003-ban látta meg a napvilágot. Ez a szabvány ötvözi a 802.11a és a 802.11b szabvány előnyeit, vagyis a 802.11a-nál elért 54 Mbit/sec elméleti sebességet értek el, a 2,4 GHz-es tartományban, megőrizve ezzel a 802.11b szabvány hatótávolságát. A 2,4 GHz-es tartománynak köszönhetően ez a szabvány visszafele kompatibilis a 802.11, és a 802.11b szabványt használó eszközökkel.

Az előnyök mellett továbbra is megmaradt a 2,4 GHz-es tartomány nagy hátránya a frekvenciatartomány foglaltsága, ugyanis ebben a tartományban működnek a mikrohullámú sütők, a vezeték nélküli vezetékes telefonok, más WLAN hálózatok, Bluetooth eszközök és még számos más eszköz. A víz saját frekvenciája is ebben a tartományban van, ami bizonyos esetekben jelenthet problémát.

Az elméleti hatótávolság beltéren körülbelül 38 m, kültéren 140 m, ami a gyakorlatban azért sokkal kevesebb. [2 pp. 24-25] [3]

1.2.5 IEEE 802.11n szabvány

A következő 802.11-es szabvány 2009-ben jelent meg, 802.11n néven. Ez az első 802.11-es szabvány, ami visszafelé kompatibilis az összes korábbi társával, mindenféle kiegészítő nélkül, ugyanis az ilyen eszközök mind a 2,4 GHz-es, mint az 5 GHz-es frekvenciatartományban működnek. A sebességet tekintve igazán nagy ugrást tapasztalhatunk, az elméleti 54 Mbit/sec után a 450 Mbit/sec, több mint 8X-os ugrást jelent. Bár a gyakorlatban ez körülbelül csak 120 Mbit/sec-ot jelent, még így is szép teljesítmény.

[7] OFDM: Orthogonal Frequency-Division Multiplexing – Ortogonális Frekvenciatartománybeli Multiplexálás

A hatótávolságot tekintve is jelentős növekedés figyelhető meg (bár a hatótávolság nagyban függ az antennától, és a router adóteljesítményétől), beltéren 70 m, kültéren 250 m elméleti hatótávolságot értek el.
Az 5 GHz-es frekvenciatartományt a 2,4 GHz-es tartomány tehermentesítése érdekében hozták vissza a gyártók, ugyan is ez az 5 GHz-es tartomány alig használt, kevesebb a zavar, így tisztább a vétel és jobb teljesítmény érhető el.
Az n szabványt használó routerek nem mindegyike képes egyszerre mind a 2 frekvencia tartományt használni, a router menüjében kell kiválasztani, hogy melyik frekvenciát kívánja a felhasználó használni, ezt a router menüjében lehet átállítani. A drágább eszközök képesek egyszerre mind a 2 frekvenciatartományban sugározni, ennek akkor van nagy jelentősége, amikor pl. sok eszköz van a routerre csatlakozva a 2,4 GHz-es sávban, és a néhány kiemelt, akik 5 GHz-en csatlakoznak, nagyobb adatátviteli sebességet érhetnek el, mint 2,4 GHz-es társaik. Fontos azonban megjegyezni, hogy nem elég adó oldalon kezelni az 5 GHz-es frekvenciatartományt, a vevő oldalon ez ugyan úgy szükséges, különben a kommunikáció nem lehetséges. [2 p. 25] [3]

1.2.6 IEEE 802.11ac szabvány

A legfrissebb 802.11-es szabvány a 802.11ac, ami tavaly, vagyis 2012-ben látott napvilágot. Az ac szabvány még az n szabványhoz képes is komoly előrelépést jelent. Az ac szabványt használó eszközök mind 5 GHz-es, mint 2,4 GHz-es tartományban is működnek, aminek köszönhetően ezek az eszközök is kompatibilisek visszafele az összes korábbi 802.11-es szabványt használó eszközzel. Az átviteli sebességben igen jelentős ugrást sikerült elérni, a 802.11ac szabványt használó eszközök 5 GHz-en 1300 Mbit/sec-os elméleti sebességet sikerült elérni, és ha ez még nem lenne elég, további 450 Mbit/sec-ot tudnak ezek az eszközök 2,4 GHz-en, és a 2 eszköz mind a 2 frekvenciasávban egyszerre is képes egymással kommunikálni. [3] [4]

2. FEJEZET: VEZETÉK NÉLKÜLI HÁLÓZATOK ESZKÖZEI

Ahogy már a bevezetésben is utaltam rá a rendszer célja, a támadó elfogása, és nem a távoltartása. Persze a hálózatot nem lehet védtelenül hagyni kiszolgáltatva minden kíváncsi szemnek, de fontos tudni, hogy nincs áttörhetetlen, vagy megkerülhetetlen védelem. A rendszer kiépítésénél azt nézik, hogy bár a szokásos védelmek a támadások jó részét megállítják, azért vannak olyan felkészült támadók, akik még így is képesek betörni a hálózatra, így ez a rendszer, egyfajta utolsó védvonalként funkcionál. A helymeghatározás viszonylagos pontossága miatt, fontos hogy a beavatkozó erők ne csak azt tudják, hogy körülbelül hol kell keresni az elkövetőt, hisz ez az információ nem elegendő abban az esetben, ha egy zsúfolt helyen próbálják megtalálni az illetőt, fontos azt is tudni, hogy mit keressenek. Természetesen olyan eszközöket, amik képesek a vezeték nélküli hálózatunkra csatlakozni, a gyanús eszközök közül pedig a technikai paraméterek és az Access Point naplózása alapján meghatározható az az eszköz, amellyel a támadást végrehajtották.

Fontos továbbá azon eszközök ismerete is, ami az épületen belül a hálózat részét képezik, hiszen ezeket az eszközöket védeni kell, mind a fizikai, mind az informatikai támadásokkal szemben.

2.1 Access Point

Az Access Point a vezeték nélküli hálózat legfontosabb eleme. Ez az az eszköz, amelyre rácsatlakozik a többi eszköz, és persze ez az eszköz fogja a támadások legnagyobb részét elszenvedni, hiszen egy jól konfigurált hálózatnál ez az „egyetlen” támadási felület.

1. kép Router
Forrás: [5]

Lakossági és kisvállalkozói környezetben az Access Point-ok elsősorban WLAN Routerek, hiszen önmagában egy vagy több számítógéppel már létrehozható vele a hálózat. Nagyobb hálózatoknál, előfordulhat, hogy az Access Point, és a Router egymástól elválik, és maradva a lakossági, és a

kisvállalkozói környezetnél, egy Bridge[8]-et használnak Access Pointnak.

Nagyvállalati, és még mikrohullámú internetszolgáltatóknál már komolyabb eszközökkel találkozhatunk, ilyenek a mikrotik és az ubiquiti eszközök.

2.2 Notebook

A támadások legnagyobb százalékánál a támadó valószínűleg notebook-ot fog használni, mert:

- Bárki számára könnyen hozzáférhetőek, az áraik pedig folyamatosan mennek lefele
- Szinte minden esetben rendelkeznek beépített WLAN kártyával
- Változatos hardver felépítésű, a kisebb teljesítményűtől egészen a csúcskategóriáig léteznek
- Mobil eszköz (akkumulátorról működtethető)
- Univerzális, gyakorlatilag bármilyen informatikai eszköz csatlakoztatható hozzá
- Könnyen telepíthető, hiszen bárhol elővehető, működtethető, és ha a helyzet úgy kívánja, könnyen elpakolható, egyszerűen össze kell csukni, és már lehet is vinni, különösen fontos ez a szempont, ha a támadó fenyegetve érzi magát.

2. kép Notebook
Forrás: [6]

2.3 Netbook

A netbookok olyan a notebookokhoz hasonló eszköz, amely kinézetre, és a felhasználhatóságot tekintve nagyon hasonlít a notebookokhoz. Mérete, számítási kapacitása kisebb, de a kisebb teljesítmény kisebb fogyasztást eredményez, így 8-10 órás üzemidő is elérhető náluk akkumulátorról. Leginkább internetezésre használhatóak, kicsi, kompakt, mobil eszközök, amelyek rendelkeznek néhány USB porttal,

3. kép Netbook
Forrás: [7]

[8] Bridge: „A hálózati híd (angolul network bridge) hálózati szegmenseket tud összekötni az OSI modell Adatkapcsolati réteg szintjén. Ethernet hálózatokban pontosan azokat az eszközöket nevezzük hídnak, amelyek megfelelnek IEEE 802.1D szabványnak.”

beépített WLAN kártyával.

2.4 Personal Computer

A személyi számítógép hasonló előnyöket rejt, mint a Notebook. Hátránya hogy nem mobil, tehát, ha egy támadó ezt az eszközt választja, valószínűleg egy szomszédos épületből követi el a támadást, telepítése időigényes, elpakolása körülményes, így valószínű, ha lebukik a támadó, akkor hátrahagyja inkább az eszközt, ami alapján beazonosítható, ezen felül anyagi kár is az elkövetőnek az eszköz elvesztése. A PC-k nem rendelkeznek beépített WLAN kártyával, de csatlakoztatható hozzájuk.

4. kép Personal Computer
Forrás: [8]

2.5 Tablet

A Tablettek, vagy táblagépek napjaink divatos eszköze, leginkább böngészésre, videó nézésre alkalmas, de képesek WLAN hálózatra csatlakozni. Hardver felépítésük változatos, a gyöngébb kategóriáktól az erősebb kategóriákig, de általánosságban elmondható, hogy kisebb számítási kapacitással bírnak, mint a Notebook-ok. Nagy előnyük a mobilitás, és a hosszú akkumulátor idő, hátrányuk hogy kevés porttal rendelkeznek, így eléggé behatárolt milyen eszközök csatlakoztathatóak még hozzá.

5. kép Tablet
Forrás: [9]

2.6 Okostelefon

Az okostelefon szintén napjaink divatos eszköze. Általánosságban elmondható, hogy számítási kapacitásban alulmúlja a tabletet, kicsi kompakt eszköz, amit könnyű előkapni, és elrakni, ugyanakkor szinte feltűnésmentesen használható, hiszen teljesen hétköznapi jelenség, hogy valaki kezében egy okostelefonnal sétál, vagy a falnak

6. kép Okostelefon
Forrás: [10]

dőlve azt használja, akár játékra, akár böngészésre.

2.7 Egyéb eszközök

Az előző pontokban azokat az eszközöket soroltam fel, amelyekről szerintem a legvalószínűbben várhatóak támadások, legyen ez akár gyenge próbálkozás, egy kis internet reményében, vagy akár komolyabb támadás adatlopás, vagy károkozás szándékával, ugyanakkor nem szabad elfelejteni, hogy a komolyabb támadások felkészült támadókat feltételeznek, ez a felkészültség pedig mind az általuk használt szoftverekben, mind az általuk használt eszközökben is megjelenhet.

További eszközök, amelyek még alkalmasak a WLAN kommunikációra:

- PDA[9]
- Digitális kamera (akár WLAN bővítőkártyával)

[9] PDA: Personal Digital Assistant

3. FEJEZET: VEZETÉK NÉLKÜLI HÁLÓZATOK FENYEGETÉSEI

A vezeték nélküli hálózatok elterjedésével „új” támadási módok jelentek meg a hálózatok ellen. Míg a vezetékes hálózatnál fizikai kapcsolat kell, hogy legyen a gép és a hálózat között (kábel), aminek a védelmét az épület maga látja el a vezeték nélküli hálózatoknál a támadó bárhonnan rácsatlakozhat a hálózatunkra az Access Point hatósugarán belül. Sajnos a hatósugár nem egy jól körülhatárolható dolog, nagyban befolyásolja a domborzat, a környező tárgyak, az adó és persze a vevő antennája. Ez igen jól megfigyelhető, ha az ember fog egy laptopot, és egy okostelefont, hogy ugyan arról a helyről a laptop a nagyobb antennája miatt erősebb jelerősséget fog mérni, nem is beszélve, ha nem a beépített gyári, hanem külön erre a célra egy nagyobb nyereségű antennát is használunk. Internetes keresgéléseim során rátaláltam egy cégre, amelynek egy úgynevezett „Netvadász készlet” az egyik termékük. A termék egy antennából, egy USB stickből, és vezetékekből áll mindössze.

7. kép: Netvadász készlet
Forrás: [11]

Magaslati pontokról létrehozott távolsági kapcsolatok Netvadász készlettel:

Tihany - Balatonfüred / 4 km / kétoldalú

Tihany - Balatonvilágos / 21 km / kétoldalú

Tokaj - Rétközberencs / 47 km / egyoldalú [11]

Persze ezek az értékek is közel ideális esetben működnek csak, szinte tökéletes optikai rálátás esetén, de még így is szép eredmény.

A vezeték nélküli hálózatok fenyegetéseit több szempont szerint lehet csoportosítani, a teljesség igénye nélkül, most csak azokkal a fenyegetésekkel foglalkozom, amelyek okozója az ember.

Az egyik ilyen csoportosítási mód a támadó személye szerint való csoportosítás, mert a támadó személye nagyjából meghatározza a motivációját, a rendelkezésre álló erőforrásokat és hogy hogyan fogja támadni a hálózatot.

3.1 A támadó személye

Dr. Muha Lajos szerint a támadók lehetnek:

- tévedő alkalmazottak
- elégedetlen alkalmazottak, vagy szerződéses partnerek
- hackerek, crackerek
- személyes előnyöket keresők (zsaroláshoz, lopáshoz)
- szervezett bűnözés ügynökei, kereskedelmi versenytársak, vagy más érdekcsoportok
- terroristák
- külföldi kémszervezetek
- ellenséges fegyveres erők [12 pp. 47-48.]

Az utóbbi kettő nem valószínű egy a piacon is szereplő magánkézben levő vállalat esetén, csak nagyon speciális esetben fordulhat elő, leginkább állami szervekre jelenthetnek fenyegetést.

Az előző felsoroláshoz tartozó fogalmak magyarázata

Hacker: A hacker az informatikai rendszerekbe informatikai eszközöket használva, kifejezetten ártó szándék nélküli betörő. Célja kizárólag a programok védelmének feltörése, kijátszása. Eredeti jelentése szerint a hacker olyan mesterember, aki fából tárgyakat farag. A tömegkommunikációban helytelenül minden számítógépes betörőre használják. [12 p. 47.]

Cracker: A cracker olyan személy, aki az informatikai rendszerekbe informatikai eszközöket használva, direkt, rombolási szándékkal tör be. A crack eredeti jelentése valami keménynek az összeroppantása, feltörése. [12 p. 47.]

Másik ilyen csoportosítási forma a támadás módja vagy informatikai eszköze szerinti csoportosítás:

3.2 A támadás módja, eszköze

- szolgáltatás megtagadás jellegű támadások
- cracking vagy hacking

- rosszindulatú programok (vírusok, férgek, trójai programok, hoaxok)
- adathalászat
- a programok hibáinak kihasználásával elkövetett betörés
- üzenetek jogtalan elfogása, lehallgatása
- belső munkatársak szándékos, vagy gondatlan károkozása
- elektronikai felderítéssel infokommunikációs rendszer adatainak a megszerzése
- egyéb elektronikai támadások[10] [12 pp. 48-49.]

Az előző felsoroláshoz tartozó fogalmak magyarázata

Cracking vagy hacking: Az informatikai rendszerekbe informatikai eszközökkel történő betörés. A Cracking minden esetben rosszindulatú, ártó vagy haszonszerzés szándékával történő betörést jelent, szemben a hackingel. [12 p. 48]

Vírusok: a számítógépes vírusok olyan programtörzsek, amelyek saját másolataikat, vagy kismértékű módosulását helyezik el („mutálódik") más programokban. Bizonyos feltételek teljesülése mellett elindul a programkódja, amely leggyakrabban romboló, néha figyelmeztető, vagy tréfás hatású. [12 p. 48]

Férgek: A férgek (Worms) olyan programok, amelyek „szaporodásukhoz" nincs szükség gazdaprogramra, önállóan szaporodnak, és fejtik ki hatásukat. [12 p. 48]

Trójai programok: A számítástechnikában a trójai programok olyan programok, amelyek valamilyen hasznos programnak „álcázzák" magukat, a felhasználó megtévesztése céljából, utalva ezzel az ókori görög mitológiából már jól ismert trójai falóra. Nem sokszorosítja magát, és nem is feltétlen tartalmaz rosszindulatú programkódot, de a legtöbb esetben tartalmaz egy ún. hátsó kaput telepítését, ami hozzáférést engedélyez a célszámítógéphez a tűzfalon keresztül. [13]

Hoaxok: A hoax angol eredetű szó, jelentése: „beugratás", „megtévesztés", „átverés", „álhír" vagy „kacsa". Olyan e-mail, amely valamely fiktív vírus terjedésére figyelmeztet, és olyan fájlok törlésére szólít fel, amelyek a számítógép működéséhez szükségesek. [14]

3.3 A támadás motivációja

Úgy vélem a vezeték nélküli hálózatok támadásainak motivációi, fő okai a következők bármelyike, vagy akár ezek közül több is lehet:

[10] Egyéb elektronikai támadások például zavarás, elnyomás.

- kihívás;
- politikai előnyszerzés;
- gazdasági előnyszerzés;
- károkozás;
- illetéktelen hozzáférés az információhoz (adatlopás);
- illetéktelen adatbevitel;
- rosszindulatú szoftverek bevitele;
- információs környezetszennyezés;
- információk megszerzése (kémkedés);
- vagyoni haszonszerzés (jogosulatlan banki átutalás);
- vagyoni károkozás (adatok törlése);
- erkölcsi károkozás (honlap megváltoztatása). [15 p. 78.]

A vezeték nélküli hálózatok támadási módszerei általános értelemben sértik az információ:

- Bizalmasságát (Confidentiality):

  Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk mértékéig ismerhetik meg, módosíthatják, vagy rendelkezhetnek felette.

- Sértetlenségét (Integrity):

  Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adat tartalma az elvárttal megegyezik, az adat megfelelő (biztonságos) forrásból származik (hitelesség), az adathoz a tárolási- és a felhasználási hely közötti térben sem fértek hozzá illetéktelenek (lehallgatás), és a rendszerelemek azon tulajdonsága, amelyek ezt lehetővé teszik.

- Rendelkezésre állását (Availability)

  Az adat, és az informatikai rendszer azon tulajdonsága, hogy az arra jogosultak az adathoz a szükséges időben, a szükséges ideig hozzáférjenek. [15 p. 79.]

Angolszász környezetben a három szó kezdőbetűiből alkotott mozaikszóval (CIA) utalnak erre a három fontos paraméterre, ezek meglétének folyamatos fenntartásának fontosságára.

3.4 A Vezeték nélküli hálózatok elleni támadások módszertana

Ebben a részben azt taglalom, hogy milyen támadási módszerekkel próbálják a támadók kijátszani a vezeték nélküli hálózatok védelmét, ezek a csoportok látszólag egymástól jól elkülönülnek, ám az elkövető általában akár tudatosan, akár tudtán kívül is ezeknek valamilyen kombinációját használja. Tudatán kívül természetesen gondatlanságból, vagy ami még valószínűbb, hogy nincs 100%-ig tisztában az általa használt szoftver működésével (pl. nem saját maga írta szoftver).

A vezeték nélküli hálózatok támadásairól már több csoportosítást is készítettek, független szervezetek, amelyek célul tűzték ki maguk elé, hogy munkájukkal a vezeték nélküli hálózatok biztonsági réseinek kutatásával növeljék azok biztonságát.

Ilyen szervezetek a CEH[11], CERT[12], IASTED[13], CISCO.

Mind a négy szervezet készített egy-egy csoportosítást, arról, hogy szerintük milyen csoportokba foglalhatóak a számítógépes hálózatok elleni támadások. Ezeket a csoportokat az 1. táblázat tartalmazza:

1. táblázat Összefoglaló táblázat a vezeték nélküli hálózatok elleni támadások csoportosításáról

	CEH	**CERT**	**IASTED**	**CISCO**	**Információs műveletek**
Passzív támadások	Felderítés	Lehallgatás	Lehallgatás	Lehallgatás	Felfedés
	Lehallgatás	Forgalom elemzés	Forgalom elemzés	Forgalom elemzés	Iránymérés
					Lehallgatás
Aktív támadás	Szolgáltatás megtagadás	Közbeékelt támadás	Szolgáltatás megtagadás	Szolgáltatás megtagadás	Elektronikai zavarás
	Megszemélyesítés	WEP, WPA kódszó törés	Megszemélyesítés	Megszemélyesítés	Elektronikai megtévesztés
	WEP, WPA jelszó törés	MAC cím visszaélés	Jogosultság kiterjesztés, lopás	Jogosultság kiterjesztés, lopás	Elektronikai pusztítás

Forrás: Saját szerkesztés

[11] CEH: Certified Ethical Hacking
[12] CERT Computer Emergency Response Team
[13] IASTED: International Association of Science and Technology for Development

A táblázatból látható, hogy mind a 4 szervezet hasonlóan vélekedik a támadások jellegéről és hogy kétszintű a csoportosításuk, mégis úgy gondolom egyikük felsorolása sem teljes, a legegyszerűbben egy összevonással, sokkal teljesebb lista összeállítható.
Az első szinten meg kell állapítani, hogy a támadás aktív, avagy passzív.

3.4.1 Passzív támadások jellemzői

A passzív támadás olyan az információ megszerzésére irányuló hálózati támadás, amely során a támadó nem vesz részt a hálózati kommunikációban, nem küld csomagokat, hanem a hozzá rádióhullámok révén eljutó nem neki címzett csomagokat fogja el, rögzíti, analizálja (lehallgatás). Titkosítatlan WLAN hálózatok esetén (pl. hotspotok) az adatok nyíltan, titkosítás nélkül utaznak AP és kliens között, így a teljes kommunikáció könnyedén kiértékelhető, így ha a felhasználó épp felhasználónevet, jelszót, vagy bankadatokat küldött egy egyszerű böngészés során azt a „fülelő" képes mindet visszafejteni. Titkosított kommunikáció esetén a visszafejtés már nehézségeket okoz, a támadónak, így ajánlott erős titkosítást, és jó jelszavat választani.

3.4.2 Aktív támadások jellemzői

Az aktív támadás olyan támadás, melynek során a támadó maga is részt vesz a kommunikációban –szemben a passzív támadással– csomagokat küld, és fogad.

3.4.3 Vezeték nélküli hálózatok elleni támadások csoportosítása

Az előbbiekben meghatároztam, hogy mi alapján dönthető el, hogy a támadás aktív, avagy passzív, ezek alapján további alcsoportokat jelölök ki:

Aktív támadások:

- Szolgáltatás megtagadása
- Középre állásos támadás (Megszemélyesítés)
- Jogosultság kiterjesztése, lopása
- Elektronikai zavarás
- Elektronikai megtévesztés
- Elektronikai pusztítás [15 pp. 79-80]

Passzív támadások:

- Lehallgatás
- Forgalomelemzés
- Iránymérés
- Felfedés [15 pp. 79-80]

3.5 Vezeték nélküli hálózatok támadási módszerei

A továbbiakban a teljesség igénye nélkül kitérek azokra a konkrét módszerekre, amelyekkel a vezeték nélküli hálózatokat támadják. Az előzőekben már kitértem arra, hogy az információ mely paramétereit kell megóvni a támadókkal szemben, itt a konkrét támadásnál kifejtem, konkrétan mely paramétert is sért a támadás.

3.5.1 Wardriving

A wardriver[14] célja a WLAN hálózatok felkutatása, és GPS[15] segítségével a GPS koordináták rögzítése, ezáltal az Access Point felfedése, és az eredmények rögzítése, és nem a hálózat feltörése, vagy a forgalmának az elemzése. A wardriving szó eredete a 80-as évekre nyúlik vissza, a nagy sikerrel bemutatott War Games (Magyarországon Háborús játékok címmel) című filmhez, amiben a főhős számítógépével találomra tárcsáz, modemekre vadászva, ez a wardialing. Ez a támadási forma, annak ellenére, hogy konkrét támadás nem történik az Access Point, vagy a WLAN-on utazó adatok ellen, igen komoly veszélyeket hordoz, hiszen a wardriverek a legtöbb esetben közzéteszik eredményeiket az interneten, ezáltal más támadók is tudomást szereznek az Access Pointunk létezéséről, védelméről.

Hardver igény:

- autó (bicikli esetén warbiking, ha a támadó gyalog van, akkor warwalking)
- WLAN antenna
- GPS készülék
- Hordozható számítógép (laptop, okostelefon, tablet)

Szoftver igény:

- Kiértékelésért felelős szoftver
- Felderítésért felelős szoftver

[14] Wardriver: Az a személy, aki a wardriving nevű „cselekményt” végrehajtja.
[15] GPS: Global Positioning System –Globális Helymeghatározó Rendszer–

Eszközök, szoftverek a támadás végrehajtásához:

- WiFiFoFum
- Inssider
- Airmon-ng
- KisMac
- MacStumbler
- NetStumbler
- Vistumbler

Ez a támadás, ha nem is az adatok lehallgatásáról, vagy az Access Point védelmének a feltöréséről szól, de elég gyakran felderítés egy másik támadás előtt.
Ez a támadási forma az adatok bizalmassága ellen irányul, hiszen az AP helye is olyan adat, amit hasznos, ha csak az arra jogosultak tudnak. [15 pp. 83-85] [16] [17]

3.5.2 Hamis AP

A támadás során a támadó, egy Access Point-ot helyez el a hálózaton, azzal a céllal, hogy lehetővé tegye saját magának a hálózatra történő bejutást. Elsősorban nagyvállalatok esetén alkalmazzák ezt a fajta támadást, ehhez azonban be kell jutni az épületbe, és egy vezetékes végpontot keresni, ahova rácsatlakozhat. Az is előfordulhat, hogy egy ott dolgozó helyezi el az AP-t, akár ártó szándékkal, önös érdekből, vagy egy más szervezetet segítve, akár csak saját kényelmét növelendő (pl. saját nem céges eszközét rá tudja kötni a hálózatra) és ha nem megfelelően konfigurálja az AP-t, védelmi rés keletkezik a hálózaton.

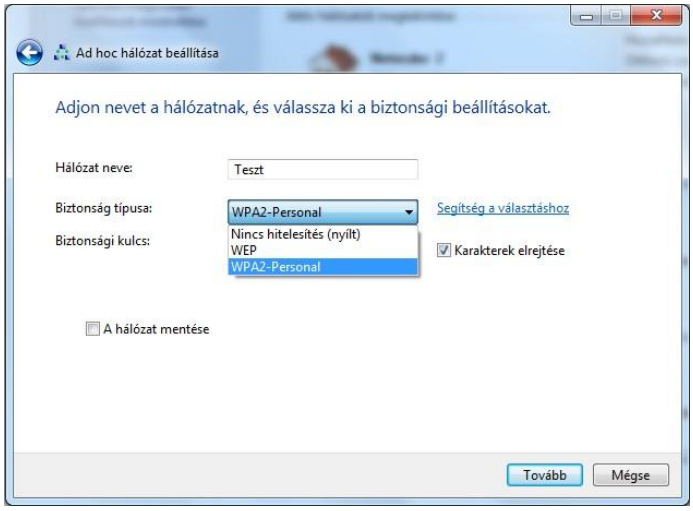
8. kép: TP-LINK Nano router
Forrás: [18]

Erre a célra bármilyen Access Point megfelel, egy router, bridge, és még sok más eszköz, a 8. és a 9. képen egy olyan eszközt mutatok, aminek már a reklámszövege is az, hogy „méretével hódít…”, és hogy „… kisebb egy bankkártyánál”.

9. kép: Méret összehasonlítás
Forrás: [18]

A 9. képről jól kivehető, hogy nem túloznak, hiszen a vastagságát leszámítva, tényleg kisebb egy bankkártyánál, így nagyon könnyen elrejthető.

Hamis AP létrehozható szoftveresen is, a Windows 7 operációs rendszer alkalmas virtuális Access Point létrehozására. A cél itt is ugyan az, mint egy igazi AP elhelyezésénél, önös érdek, egy támadó csoport segítése, vagy csak kényelmi funkciók. Abban az esetben, ha az elkövetőnk, aki beállítja ezt a kapcsolatot, ott dolgozó, és semmilyen ártó szándék nem vezérli, akkor is egy védelmi rés keletkezik a hálózaton, elvégre a hálózat feltételezhetően egy jól konfigurált hálózat, míg ez az AP csak annyira biztonságos, amennyire az illető beállítja. Ha nem ért hozzá, akkor lehet, hogy nem is állít be titkosítást, mert úgy kényelmesebb, még akkor is, ha a varázsló felkínálja a WEP és a WPA2 titkosítást is.
A következő kép egy ilyen AP létrehozásának a beállításait mutatja:



10. kép Ad hoc kapcsolat beállításai

Forrás: [Saját szerkesztés]

Ahogy a neve is mutatja, Ad hoc hálózat, vagyis alkalmi hálózat, amely magában hordozza, hogy nem annyira professzionális, mint az olyan eszközök, amelyeket erre készítettek.
Mindazonáltal nem igényel plusz hardvert, vagyis plusz költséget, és nem utolsósorban nem kell elrejteni sem.
A támadás eszközigénye ezek alapján bármilyen szoftveres, vagy hardveres AP, és mivel a hálózathoz való hozzáférést segíti egy támadónak, így az adatok bizalmasságát sértik. [15 pp. 86-88.]

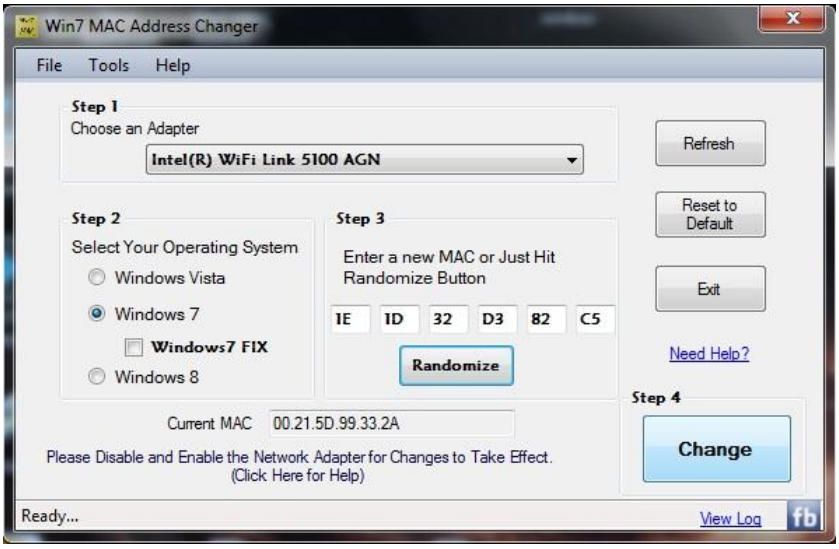
3.5.3 MAC[16] csere

A MAC cím, vagy más néven Fizikai cím a hálózati kártya egyedi azonosítója, amely minden eszköznek egyedi, a gyárban megadott érték. A MAC cím hat részből áll, egymástól kettősponttal elválasztva, és minden rész egy két számjegyű hexadecimális szám.

Pl.: 00:1B:44:11:3A:B7

Ezt az azonosítót –mivel elméletileg minden hálózati eszköz sajátja, és nem megváltoztatható– gyakran használják a hálózat használatára jogosult eszközök azonosítására.

Abban az esetben, ha a hálózatot más módon nem védik, egy támadónak mindössze annyi a dolga, hogy lehallgatja az AP és egy kliens kommunikációját, ebből megtudja a MAC address-ét a kliensnek, és amikor nem forgalmaz, bejelentkezik a kliens MAC címével.



11. kép MAC Address Changer

Forrás: [Saját szerkesztés]

Komolyabb védelemmel ellátott hálózatok esetén ahol az azonosításnak több kritériuma is van, nem elégséges pusztán a MAC cím cseréje, de szükséges, és ez is egy lépés a támadónak a hálózat feltöréséhez.

Eszközigény: olyan szoftver, amely alkalmas a MAC cím cseréjére.

Ez a támadási forma a hozzáférés elleni támadások közé tartozik. [15 pp. 85-86.]

[16] MAC: Media Access Control

3.5.4 Add Hoc csatlakozás

A támadás során a támadó egy rosszul konfigurált, vagy direkt erre a célra telepített AP-t, vagy rajta keresztül az egész hálózatot támadja.

Eszközigény: WLAN hálózati kártya

Ez a támadási forma a hozzáférés elleni támadások közé tartozik.

3.5.5 Lehallgatás

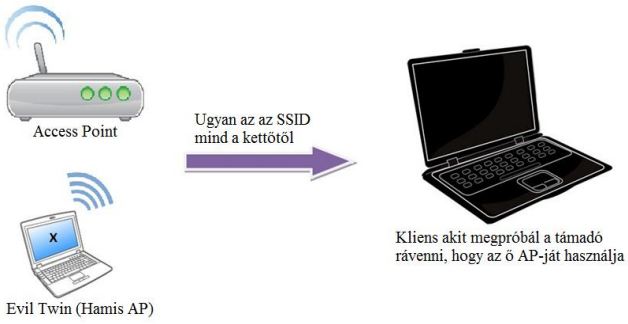
Ennél a támadási formánál a támadó a hálózat hatósugarán belül tartózkodik, és a kommunikációs csomagokat igyekszik elkapni. Titkosítatlan hálózat esetén a nyíltan utaznak az adatok az AP és a Kliens között, így dekódolásra sincs szükség. Titkosított kommunikáció esetén is kiértékelhető megfelelő számú csomag esetén, de ez már jelentősen megnehezíti a támadó dolgát.

Eszközigény: a legtöbb WLAN kártya nem alkalmas erre a funkcióra, így olyan kártya, vagy stick kell, ami erre alkalmas.

Ez a támadási forma a bizalmasság elleni támadások közé tartozik.

3.5.6 Evil Twin

Evil Twin más néven gonosz iker. A támadás lényege, hogy a támadó lemásol egy AP-t, (SSID, jelszó), és valahogy megpróbálja elérni, hogy a kliensek inkább az ő AP-jára csatlakozzanak fel, olykor ezt az AP kicserélésével érik el.



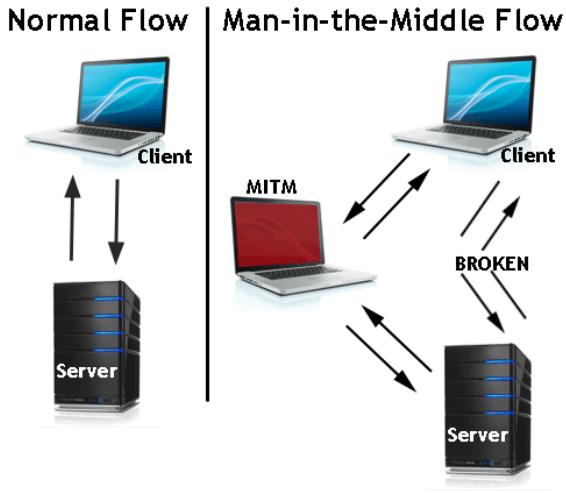
12. kép: Evil Twin támadás
Forrás: [19]

Ezzel a módszerrel a teljes hálózati forgalmat monitorozni bírják, leginkább felhasználónevek, jelszavak ellopására használják, de alkalmas hitelkártya adatok ellopására is. [20]

3.5.7 Man in the Middle

A Man in the Middle vagyis közbeékelt támadás az Evil Twin továbbgondolt változata, amely során nemcsak elhelyez egy AP-t a támadó, hogy arra csatlakozzanak a kliensek, hanem a kommunikációt vissza is tereli az eredeti AP-re, persze csak rajta keresztül. A

támadás veszélye, hogy az egyetlen dolog, amit észrevehet ez a támadás során a felhasználó, hogy a hálózat sebessége csökken (ha csökken). [15 p. 90.]



13. kép: Man in the Middle támadás

Forrás: [21]

3.6 Vezeték nélküli hálózatok védelmi módszerei

Az előzőekben megismerkedtünk számos olyan módszerrel, amellyel illetéktelen személyek megpróbálhatnak hálózatunkra rácsatlakozni, vagy bármilyen más módon adatokat ellopni.

A dolgozat következő részében arról lesz szó, hogy a rendszergazdák hogyan védekeznek ezekkel a támadásokkal szemben. A védelem megvalósítása több szintű szoftveres, és hardveres eszközökkel megvalósítható, hogy az ember mit választ, a védelmi igény, és az árak határozzák meg. Bármilyen védelem kiépítésénél, legyen az WLAN hálózat, vagy csak egy egyszerű családi ház, autó, vagy bármi más, fontos szem előtt tartani, hogy:

- a védelem ne kerüljön többe, mint az az érték, amit védeni szeretnénk.
- mivel manapság már mindenre van valami megoldás, bármilyen védelmet is építünk ki, az feltörhető, áttörhető, vagy megkerülhető, a védelemnek ki kell tartania ameddig a támadás tényére fény derül, és ameddig a szükséges intézkedések végrehajthatók.

A vezeték nélküli hálózatok védelmi módszereit elsősorban az alapján lehet csoportosítani, hogy a védelmi módszer aktív, avagy passzív.

A **passzív védelmi módszerek**, olyan a hálózatot védő módszerek, amelyek folyamatosan működnek, független attól, hogy a hálózat épp egy támadás alatt áll, avagy nem, és csak a jogosult személyeket engedik be a hálózatra:

- vírusirtó
- tűzfal
- hozzáférés szabályozás
- behatolás észlelés
- az eszközök, és végpontok fizikai védelme

14. kép: Access Denied (belépés megtagadva) Forrás: [22]

Az aktív védelmi módszerek olyan a hálózatot védő módszerek, amelyek olyankor működnek, amikor a hálózat támadás alatt áll, céljuk a támadó eltántorítása, megzavarása:

- megelőző támadások
- ellentámadás
- aktív megtévesztés

Bármilyen WLAN hálózatról is legyen szó, hacsak nem az a célunk, hogy bárki számára könnyen elérhető és használható legyen (pl. hotspotok) a hálózatot, az Access Pointot, és a rajta folyó adatokat védeni kell, ehhez az alábbi módszereket javaslom:

Passzív védelem:

- Erős hitelesítés, és titkosítás
- SSID nevének megfelelő megválasztása és vagy elrejtése
- MAC cím szerinti szűrés
- Működési idő szabályozása (amennyiben ez megoldható, a felhasználást nem gátolja)
- Access Point(ok) helyének gondos megválasztása

Az előbbi megoldások mindegyike olyan opció, amely nem jelent anyagi terhet senkinek, hiszen a mai Access Pointok mindegyike tudja már, mindössze beállítás kérdése az egész, így mindenki számára ajánlott. Akinek még ennél is komolyabb

védelemre van szüksége, az alábbi passzív védelmi módok állnak még rendelkezésére, amelyek már beruházást igényelnek.

- Antennák megfelelő méretezése
- Hálózati forgalom monitorozása
- Naprakész vírusirtók, operációs rendszerek
- Tűzfal használata a hálózat különböző szegmensei között
- Behatolás érzékelő szoftverek

Aktív védelem:

Az aktív védelmi módok mindegyike beruházást igényel, de igen hasznosak tudnak lenni:

- Megtévesztő rendszerek
- Ellentámadó rendszerek

4. FEJEZET: HELYMEGHATÁROZÁS MÓDSZERTANA

A rádióhullámokkal történő helymeghatározásnál/távolságmérésnél a rádióhullámok szinte minden fontos tulajdonságát kihasználják. A rádióhullámok terjedési sebessége – megegyezik a fény terjedési sebességével, vagyis megközelítőleg $3*10^8$ m/s– a frekvencia –másodpercenkénti rezgésszám (Hz)– és az intenzitás (dBm) azok a legfontosabb paraméterek, amelyeket a mérések során figyelembe vesznek.
A rádiólokáció alapvetően kétféle módon működik:

- időméréssel
- jelintenzitás méréssel

A mérés jellegét tekintve lehet:

- aktív
- passzív

A lokalizáció aktív, avagy passzív jellege attól függ, hogy a mérés során a mérést végző eszköz, küld e ki rádióhullámokat, vagy csak fogadja (lehallgatja) őket.

Aktív rádió lokalizáció esetén a mérést végző eszköz rádióhullámokat küld ki, amelyek ha egy tárgyba ütköznek, visszaverődnek róla. A jel kibocsátása, és fogadása között eltelt idő, a visszaverődött jel intenzitása, esetleges frekvenciamodulációkból lehet következtetni a tárgy távolságára, alakjára, mozgásának sebességére, irányára.

Passzív rádió lokalizációról abban az esetben beszélünk, amikor a mérést végző eszköz egy rádióhullámokat sugárzó tárgy/eszköz által sugárzott jelet fogadja, és ebből határozza meg a tárgy/eszköz helyét.

A továbbiakban csoportokat képzek az előző két csoportból, és így bemutatom a konkrét működési módokat:

4.1 Aktív rádiólokáció időméréssel

Az ilyen módon történő rádiólokációnál egy rádióadó segítségével rádióhullámokat bocsátanak egy célterületre, és az ott elhelyezkedő tárgyakról a rádióhullámok nagy

része visszaverődik. Ezt a visszaverődő jelet egy rádióvevő fogja fel, a kibocsátás, és a visszaérkezés között eltelt időből számolják ki a tárgy távolságát.
A fizikából már jól ismert v=s/t képletet átrendezve:

$$s=v*t$$

ahol „s” a tárgy távolsága, „v” a rádióhullámok sebessége, „t” a kibocsátás, és a visszaérkezés között eltelt idő fele.
Ezzel a módszerrel kiszámítható az ADÓ/VEVŐ és a tárgy közötti távolság, bár így konkrét helyet nem tudunk meghatározni, egy gömb sugarát kapjuk meg, melynek felületén bárhol elhelyezkedhet a céltárgy, de 4 ADÓ/VEVŐ párossal a gömbök közös metszéspontja a „pontos” helyet meghatározza.
Ezen az elven működik az aktív RADAR.

4.2 Passzív rádiólokáció időméréssel

Ennél a módszernél az adó és a vevő elválik egymástól, az adó már nem csak egyszerű rádióhullámokat bocsát ki, hanem elküldi a vevőnek a küldés pontos idejét is. A vevő a regisztrálja a rádióhullámok érkezésének idejét, és összehasonlítja az adó által elküldött idővel, vagyis, hogy mikor küldte. A kettő közötti különbség a rádióhullámok utazási ideje.

$$t_{küldött}-t_{fogadott}=t$$

A továbbiakban a helymeghatározás menete ugyan az, mint az előző módszernél:

$$s=v*t$$

ahol „s” az ADÓ és VEVŐ közötti távolság, „v” a rádióhullámok sebessége, és „t” az előző módszerrel kiszámított idő.
Az „s” jelen helyzetben is egy gömb sugara, az ADÓ körül, vagyis 4 adó segítségével a „pontos” hely meghatározható.
Ezen az elven működik a GPS.

4.3 Passzív rádiólokáció jelintenzitás méréssel

Ennek a helymeghatározási módszernek alapvetően 2 változata létezik, a két változat abban egyezik meg egymással, hogy az ADÓ és a VEVŐ egymástól teljesen elkülönül, és a beérkező jelek intenzitását mérik.

4.3.1 Passzív rádiólokáció jelintenzitás méréssel, irányított antennával

Az irányított antenna segítségével a legnagyobb jelszintet megkeresve a keresett eszköz az antennától számított képzeletbeli vonalon fekszik. Távolság mérésére így nem alkalmas, maximum a távolság megbecsülésére. Több irányított antenna felhasználásával ezek a képzeletbeli vonalak egy pontban metszik egymást, a keresett eszköz azon a ponton található.

Ezzel a módszerrel csak olyan objektumok helye meghatározható, amelyek rádióhullámokat sugároznak.

Ezen az elven működik a passzív RADAR.

4.3.2 Passzív rádiólokáció jelintenzitás méréssel, körsugárzóval

Ez módszer ismert helyen elhelyezett körsugárzókat használ, amik a nevükkel ellentétben a helymeghatározáshoz nem sugároznak, hanem csak jelet fogadnak, a rádióhullámokat sugárzó objektumok helyének meghatározására. Az egyes antennák valamekkora intenzitással fogják az objektum által sugárzott jelet, és az antennák helyének, és a jelerősségek ismeretében becsülik meg az objektum helyét.

Ezt a módszert mobiltelefonok helyének meghatározására használják, ahol a telefon a keresett objektum, a mobilszolgáltatók tornyai a körsugárzók.

A rádióhullámokkal történő összes helymeghatározás a fenti elvek valamelyikén működik, így a szakdolgozatom további részében ezek közül a módszerek közül próbálok átültetni WLAN hálózatokra egy vagy több módszert, annak érdekében, hogy lokalizálhatóak legyenek a vezeték nélküli hálózatok támadói.

5. FEJEZET: KONKRÉT MÓDSZER KIDOLGOZÁSA A VEZETÉK NÉLKÜLI HÁLÓZATOK TÁMADÓINAK A LOKALIZÁLÁSÁRA

Ezzel a fejezettel el is jutottam az utolsó és egyben legfontosabb célhoz, amelyet célul tűztem ki magam elé a szakdolgozatom megírásánál, vagyis lokalizálni egy vezeték nélküli hálózat támadóját.

Ahogy már az 4. fejezetben említettem, azon módszerek valamelyikét, vagy akár többet is próbálok meg átültetni vezeték nélküli hálózatokra, ezek elvi megvalósítása számos nehézséget, elvi hibát, és technikai kihívást okoz, mivel arra a konkrét területre vannak kifejlesztve, optimalizálva, arról nem is beszélve, hogy azok a technológiák már jól működő kiforrott technológiák.

5.1 Nehézségek a vezeték nélküli hálózatok támadóinak lokalizálásánál

Ebben a részben kifejtem azokat a dolgokat, amelyeket mindenképp szem előtt kell tartanom, a rendszer tervezésénél, kivitelezésénél, és persze azoknak is mindenképp szem előtt kell ezeket tartani, akik ugyan ezen a kutatási területtel fognak foglalkozni.

5.1.1 A rádióhullámok sebessége

A rádióhullámok sebessége állandó, a fény sebességével megegyező érték, megközelítőleg $3*10^8$ m/s. A rádióhullámok sebességének előny, és hátrány is egyben.

Ez a sebesség előny abból a szempontból, hogy elég sok mérés elvégezhető rövid idő alatt, a sok mérés pedig mindenképp pontosságot növelő tényező.

A feldolgozást, és a mérést mindenképpen számítógép végzi. A számítógép processzora jó esetben többmagos, de általánosságban feltételezhető, hogy a gép processzorának a sebessége, 1,5 GHz és 3 GHz közé esik (polgári felhasználás esetén, nem polgári felhasználásban, ennél jobb is előfordulhat). Ha veszünk egy 2 GHz-es processzort, az a processzor $2*10^9$ műveletet képes elvégezni másodpercenként, vagyis 1 művelet 0,5 ns alatt végez el. A fény ennyi idő alatt 15 cm-t tesz meg, vagyis, ha a processzor képes lenne minden műveletre feldolgozni a jelet, 15 cm pontosság lenne elérhető. Valójában a processzornak mást is kell számolni, futtatni az operációs rendszert, más programokat,

és maga a feldolgozás is több műveletet vesz igénybe, így ez a pontosság közel sem megvalósítható.

5.1.2 Az Access Point hatótávolsága

A vezeték nélküli hálózatok hatótávolságát már a 2.2-es fejezetben érintettem az IEEE szabványok felsorolásánál. A helymeghatározás minden fajtájánál, amelyek már működnek, nagy távolságokról beszélünk, akár a RADAR-ról beszélünk, akár a GPS-ről, akár bármi másról, a vezeték nélküli hálózatoknál viszont 50 m-en belüli távolságokról, körsugárzó esetén, optikai rálátás esetén, ideális körülmények között, mehetünk csak el akár 100 m-ig.

5.1.3 Kliensek hatótávolsága

Mivel 2 oldalú kommunikáció csak akkor jöhet létre, ha mind a 2 fél látja egymást, a hatótávolság minden esetben a gyengébb eszköz hatótávolsága. Már korábban is utaltam rá, hogy az egyes eszközök hatótávolsága eltér egymástól, függ a kliens antennájától, és az adóteljesítménytől.

5.1.4 A rádióhullámok verődése, - elnyelődése

Mint tudjuk, a rádióhullámok a legtöbb általunk használt anyagon áthatolnak, falon, műanyagon, fán, stb. ezért roppant kényelmes a használatuk. Az is tapasztalati tény, hogy a jelerősség gyengül, ha egy tereptárgyat teszünk az ADÓ és a VEVŐ közé, ennek oka, hogy a rádióhullámok csak egy része halad át ezeken az anyagokon, más része visszaverődik a felületről. A visszaverődést tekintve a rádióhullámok ugyan úgy viselkednek, mint a fény, vagyis:

- a beeső hullámok, és a visszavert hullámok egy síkban vannak
- a beesési-, és a visszaverődési szög egyenlő

A rádióhullámok verődéséből az a tény következik, hogy egy iránymérésnél előfordulhat, hogy a legerősebb jel nem a jelt kibocsátó tárgy felől érkezik, hanem visszaverődések egész sorozatát követően egy másik, akár ellentétes irányból. [23]

Ezek alapján bármilyen rádióhullámok segítségével történő helymeghatározó módszernél a rádióhullámok az alábbiakban felsorolt tulajdonságait figyelembe kell venni, és számolni kell a mérésekben megjelenő hatásukra.

5.2 Vezeték nélküli hálózatoknál a helymeghatározásra alkalmas módszerek

Az 4. fejezetben felsorolt módszerek közül véleményem szerint 3 módszer alkalmas egy támadó helyének a lokalizálására. Mind a három módszer alapos végiggondolása, és mérések elvégzése után a következőkre jutottam:

5.2.1 Aktív lokáció időméréssel

Ez volt az első módszer, amellyel foglalkoztam, mivel a legígéretesebb tűnt mindközül. Ahogy már utaltam erre, ezzel a módszerrel a RADAR-ok mérnek, jeleket bocsátanak ki, amelyek a céltárgyakról visszaverődnek, és a kibocsátás és a visszaérkezés között eltelt időt mérik.

Informatikai rendszerekben ez a módszer a következő lépések szerint működne:

1. A támadó sikerrel rácsatlakozott az Access Pointra.
2. A mérést végző számítógép csomagokat küld a feltételezett támadó gépre, amely válaszol ezekre a csomagokra, a küldés, és a fogadás között eltelt idő mérésre kerül.
3. A mérést végző számítógép az Access Point fele ugyan ezt a mérést elvégzi.
4. Az 1. lépésnél, és a 2. lépésnél kapott értékeket ki kell vonni egymásból, és osztani kell 2-vel, így megkapjuk, azt az időt amennyi idő alatt a csomagok megérkeztek az AP-tól a támadó gépig, vagy fordítva.
5. Ezt a mérést 4 különböző helyen elhelyezet körsugárzóval el kell végezni, a körsugárzók elektronikus eszközökkel leválaszthatók, és csatlakoztathatók az AP-hoz.
6. Az adatok kiértékelése, megjelenítése

A módszert a gyakorlatban is kipróbáltam, egy Access Point és a bele integrált körsugárzó felhasználásával és a mérés során következő adatokat kaptam.

A mérés leírása:

A mérés célja szimulálni egy a vezeték nélküli hálózat elleni támadást, amely során, a támadó, már áttörte a hálózat védelmét, és bejutott a hálózatra. A mérést végző számítógép a „ping -t” paranccsal folyamatosan „ping”-eli először a támadó eszközt,

majd az Access Point-ot, 32 bájtnyi adattal. Két mérést végeztem el, melynek során a támadó eszköz vezeték nélkül csatlakozik a hálózathoz, a mérést végző eszköz pedig az egyik esetben vezeték nélkül, a másik esetben pedig LAN-on keresztül csatlakozik az Access Pointhoz.

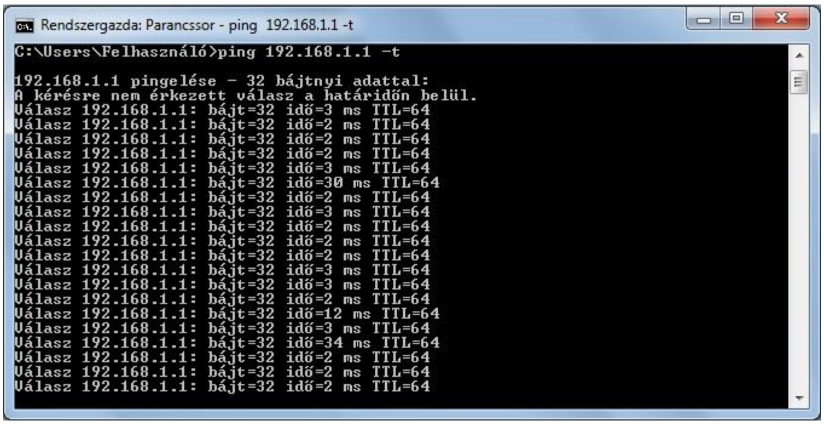
A méréshez használt eszközök és a hálózaton betöltött szerepük:

- Mikrotik RouterBOARD 951G-2HnD (Access Point)
- ASUS M51VR Notebook (Mérést végző eszköz)
- Samsung Galaxy Ace okostelefon (Támadó eszköz)
- UTP kábel

Mérési elrendezés:

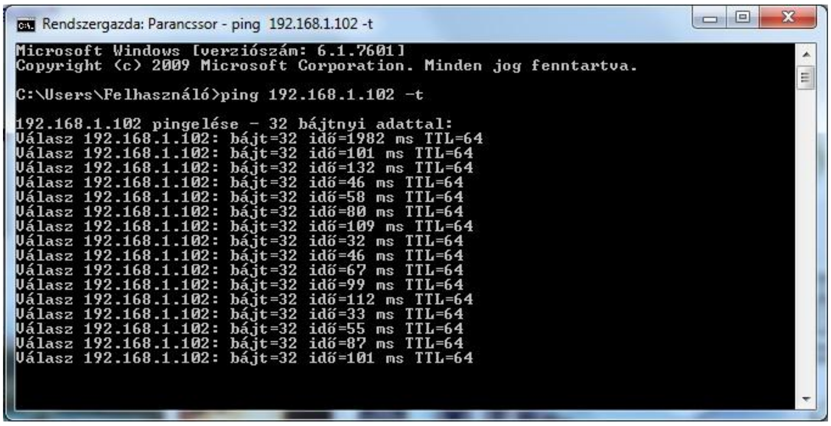
15. kép: Aktív lokáció időméréssel mérési elrendezése
Forrás: Saját szerkesztés

A mérési eredmények a következő képeken láthatóak:



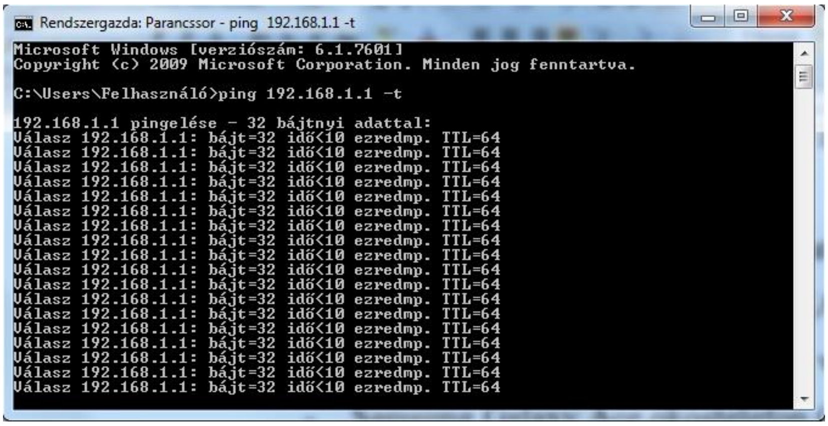
16. kép Access Point pingelése WLAN-on

Forrás: Saját szerkesztés



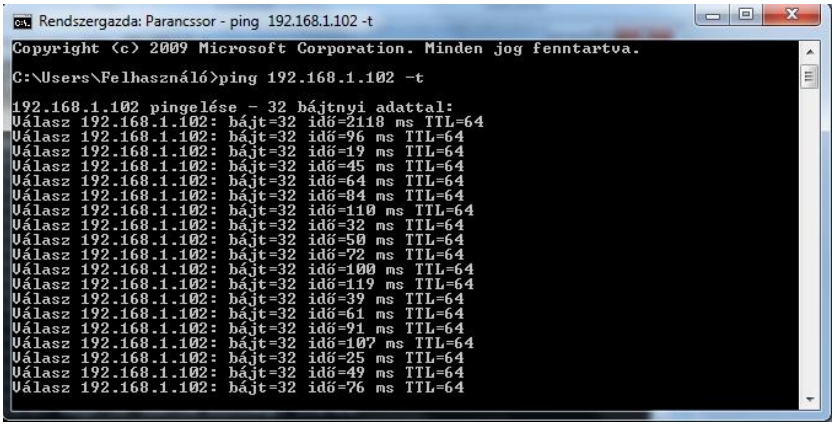
17. kép Támadó pingelése WLAN-on

Forrás: Saját szerkesztés



18. kép Access Point pingelése LAN-on

Forrás: Saját szerkesztés



19. kép Támadó pingelése LAN-on

Forrás: Saját szerkesztés

Konklúzió:

A mérési eredmények sajnos még csak viszonylag sem egységesek, a válaszidők elég széles tartományban mozognak, ráadásul, ha a rádióhullámok sebességéhez viszonyítjuk, 1 ms is nagy eltérés. A továbbiakban ezzel a módszerrel nem foglalkozom, nem tartom kizártnak, hogy valaki valamilyen hasonló módszerrel sikerrel jár, ezért is vettem a lehetséges módszerek közé.

5.2.2 Passzív lokáció jelintenzitás méréssel, irányított antennával

Az irányított antennával történő jelintenzitás méréssel rádióhullámokat sugárzó objektumok helye határozható meg, oly módon, hogy az irányított antenna forgatásával a legerősebb jelintenzitást irányába kell fordítani (lásd. 4.3.1). Célszerű minél szűkebb karakterisztikájú antenna használata, mert így pontosabb a mérés.

Informatikai rendszerekben, ez a módszer a következőképp működik:

1. A támadó sikerrel rácsatlakozott az Access Pointra
2. A mérést végző számítógép megfelelő automatika segítségével irányított antennákat (minimum kettőt) mozgat, amelyek csak vevő üzemmódban működnek, és a legerősebb jelintenzitást keresik.
3. Az antennák irányvonalainak a metszete meghatározza a támadó helyét

A módszert a gyakorlatban is kipróbáltam, egy Access Point, és egy irányított antenna felhasználásával, és a mérés során a következő eredményekre jutottam:

A mérés leírása:

A mérés célja szimulálni egy vezeték nélküli hálózat elleni támadást, amely során a támadónak sikerült bejutni a hálózatra. A mérés során a mérést végző számítógéphez AirPcap sticken keresztül csatlakoztattam irányított antennát és Wireshark nevű program segítségével analizáltam a támadó eszköz által küldött csomagokat, és mértem a jelintenzitást két különböző helyről.

A mérést beltéren, és kültéren is elvégeztem.

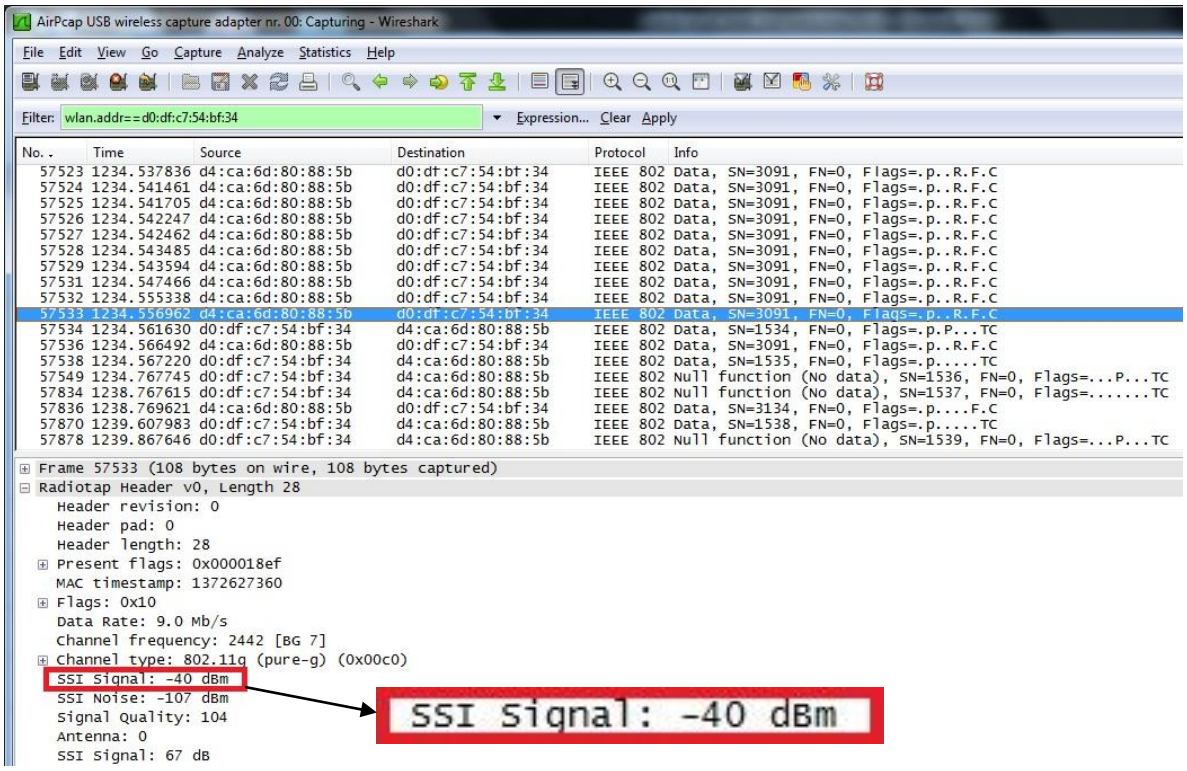
A méréshez használt eszközök és a hálózaton betöltött szerepük:

- Mikrotik RouterBOARD 951G-2HnD (Access Point)
- ASUS M51VR Notebook (Mérést végző eszköz)
- Samsung Galaxy Ace okostelefon (Támadó eszköz)
- AirPcap stick
- Irányított antenna

Mérési elrendezés:

20. kép: Passzív lokáció jelintenzitás méréssel, irányított antennával
Forrás: Saját szerkesztés

Mérés beltéren:
A mérést beltéren kétféleképp végeztem el, az első lépésben az irányított antenna, és a támadó készülék egy szobában volt. A szoba 2 különböző pontjából ki tudtam mérni a legerősebb jelerősségeket, és meghatározni a készülék antennától számított irányát.
A mérés során a legerősebb jelek a készülék irányából jöttek, megjegyzendő azonban, hogy a beltér, és a jel verődése miatt egy-két „erős” kósza jel impulzusszerűen más irányból is érkezett, de a készülék irányából stabil erős jelek érkeztek.



21. kép: Pillanatkép a Wireshark nevű programból
Forrás: Saját szerkesztés

A mérést beltéren úgy is elvégeztem, hogy a támadó eszköz a szomszéd szobában volt elhelyezve, a mérés során a több pontról történt mérés ellenére azonos eredményeket kaptam, a két szoba közötti ajtó felől, érkeztek a legerősebb jelek. Ennek szintén a jel verődése és - elnyelődése az oka, hiszen a falon keresztül érkező jelek egy része elnyelődik, így az ajtó felől, ahol nem nyelődik el, csak verődik, érkeznek a legerősebb jelek.

Mérés kültéren:
A mérés során 4 dobozt helyeztem el, egymástól 2 m távolságra, egyvonalban, és egy második személy segítségét kértem, hogy helyezze el a telefont az egyik dobozba.

Két mérést végeztem el, két különböző helyről, és mind a két mérés ugyanarra a dobozra mutatott amelyik dobozban a telefon volt.

Konklúzió:
A mérés az általam remélt eredményeket hozta, vagyis, hogy irányított antennával valóban meg lehet határozni egy WLAN eszköz helyét amikor az rá van csatlakozva a hálózatra. A módszer csak kültéren működik, beltéren nem javaslom az alkalmazását.

5.2.3 Passzív lokáció jelintenzitás méréssel, körsugárzóval

A körsugárzóval történő helymeghatározás esetén a rádióhullámokat kibocsátó objektum helye, az ismert helyen elhelyezett körsugárzók és a jelintenzitás ismeretében becsülhető meg (lásd. 4.3.1). A minél pontosabb eredmény, és a minél nagyobb hatótávolság érdekében célszerű minél nagyobb nyereségű antennák használata.
Informatikai rendszerekben, ez a módszer a következőképp működik:

1. A támadó sikerrel rácsatlakozott az Access Pointra
2. A mérést végző számítógép egy kapcsolórendszeren keresztül csatlakoztatja magához, és választja le az antennákat (egyszerre csak egy antennával mér).
3. A fogott jelek intenzitásának összehasonlításából megbecsülhető az eszköz helye.

A mérés leírása:

A mérés célja szimulálni egy vezeték nélküli hálózat elleni támadást, amely során a támadónak sikerült bejutni a hálózatra. A mérés során a mérést végző számítógéphez AirPcap sticken keresztül csatlakoztattam körsugárzót és Wireshark nevű program segítségével analizáltam a támadó eszköz által küldött csomagokat, és mértem a jelintenzitást az épület több pontján.
A mérést csak beltéren végeztem el.

A méréshez használt eszközök és a hálózaton betöltött szerepük:

- Mikrotik RouterBOARD 951G-2HnD (Access Point)
- ASUS M51VR Notebook (Mérést végző eszköz)
- Samsung Galaxy Ace okostelefon (Támadó eszköz)
- AirPcap stick
- Körsugárzó

Mérési elrendezés:

22. kép: Passzív lokáció jelintenzitás méréssel, körsugárzóval
Forrás: Saját szerkesztés

A mérés során a támadó eszköz elhelyezésében külső segítséget kértem, mivel ha nem tudom az eszköz helyét, a személyes benyomásaim nem befolyásolják a mérés kimenetelét.

Az épület alaprajza az 1. mellékletben látható:

2. táblázat: Passzív lokáció jelintenzitás méréssel, körsugárzóval mérés mérési eredményei:

	Szoba megnevezése	Mérési eredmény (dBm)	Következtetés
1. mérés	Konyha	~ - 80	-
2. mérés	Előtér	~ - 76	Közeledek az eszközhöz
3. mérés	Nagyszoba	~ -53	Közeledek az eszközhöz
4. mérés	2. szoba	~ -87	Távolodok az eszköztől
5. mérés	Folyosó	~ - 83	*
6. mérés	Kisszoba	~ -96	Távolodok az eszköztől

Forrás: Saját szerkesztés

* A vékonyabb falak okozhatják a jel erősödését

Konklúzió:

Ahogy a mérési eredmények is mutatják, az eszköz a nagyszobában volt. A gyenge jelerőség a továbbiakban zavaró lehet, ennek oka, hogy a támadó eszköz egy okostelefon, amelynek méreteiből adódóan, kicsi az antennája, és alacsony az adóteljesítménye. Mindent összevetve, a mérés az általam várt eredményeket hozta, vagyis helyiségszinten meg tudtam vele határozni egy WLAN eszköz helyét, miközben az egy WLAN hálózatra van csatlakozva.

5.3 Konkrét módszer kidolgozása a vezeték nélküli hálózatok támadóinak a lokalizálására és a rendszerelemek ismertetése

A vezeték nélküli hálózatok támadóinak a lokalizálása olyan komplex feladat, amely komplex megoldást igényel, megvalósításához összetett rendszer szükséges, aktív- és passzív védelmi elemekkel, melyben minden rendszerelemnek megvan a saját maga feladata. Ahogy már a korábbiakban is leírtam, ezt a rendszert a hálózat egy utolsó

védvonalának terveztem, azok a támadók ellen, akik elég felkészültek, és képesek a hálózatra való bejutásra, és nem minden apró kis próbálkozás ellen, amely a hálózatot ér. Kétségtelen, hogy a rendszer az ilyen apróbb támadások felderítésére is használható lenne, de az ilyen komolytalan próbálkozások miatt kár terhelni mind a rendszergazdát, mind a beavatkozó személyzetet.

Az általam tervezett rendszer működése az alábbi módon írható le:

1. Alaphelyzet: a hálózatot jogosultan használók kiszolgálása, gyenge támadások kivédése
2. Riasztás: aktív megtévesztés, személyzet értesítése az eseményről
3. Helymeghatározás: a támadó helyének meghatározása
4. Visszaállás alaphelyzetbe: A veszély elmúltával visszaállás az alap helyzetbe

5.3.1 „Gyenge" támadások kivédése

A „gyenge" támadások kivédésére gyakorlatilag bármilyen Access Point képes, és olyan passzív védelmi módszereket sorolok ide, amelyek nem kerülnek semmilyen többletköltségbe a tulajdonosnak mindössze beállítás kérdése az egész.

5. Erős hitelesítés, és titkosítás
6. SSID nevének megfelelő megválasztása és vagy elrejtése
7. MAC cím szerinti szűrés
8. Működési idő szabályozása (amennyiben ez megoldható, a felhasználást nem gátolja)
9. Access Point(ok) helyének gondos megválasztása

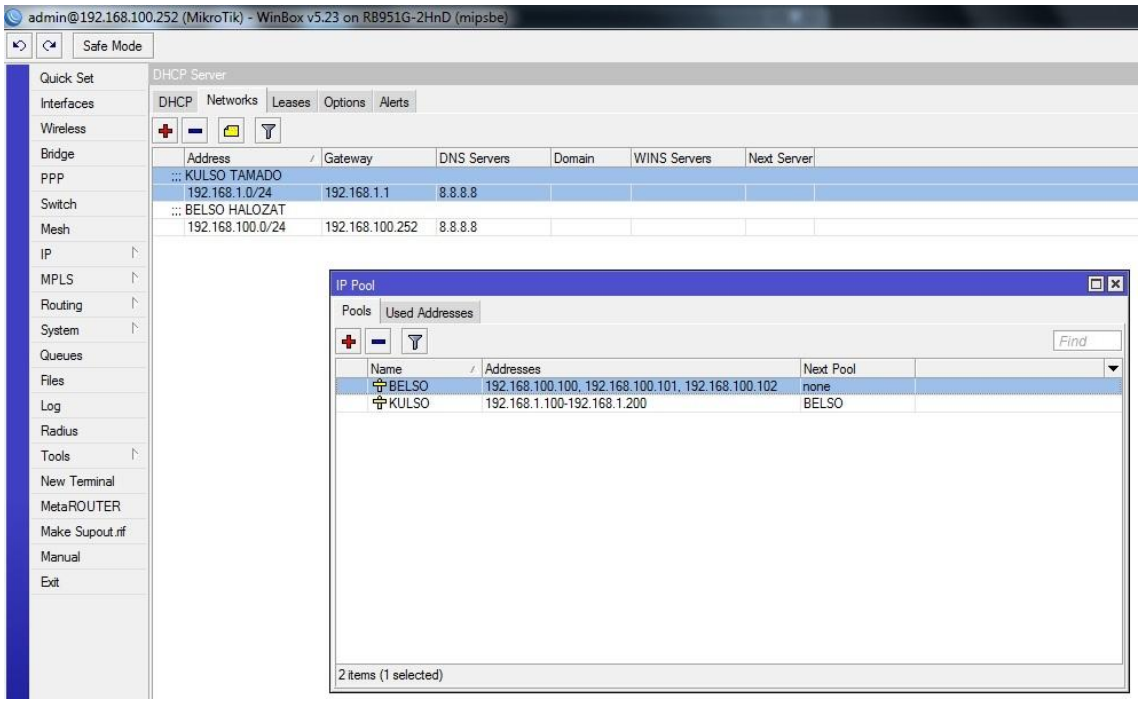
5.3.2 Aktív megtévesztés

Az aktív megtévesztés a védelem következő lépcsőfoka, abban az esetben, ha a támadónak sikerült rácsatlakozni az Access Pointra, száműzhető egy olyan térbe, ahol nem tud semmilyen kárt tenni, vagyis egy úgynevezett „homokozó"-ba, vagy „honeypot"-ba (magyarul: mézes bödön). A támadó „honeypot"-ba való száműzése úgy is megvalósítható, hogy közben a hálózatot jogosan használók továbbra is megszakítás nélkül használhassák azt, mégse legyenek egymásnak felderíthetőek a támadó -, és a hálózatot jogosan használó eszközök, annak ellenére, hogy ugyan arra az Access Pointra vannak rácsatlakozva és az Access Point ugyan azt az SSID-t küldi mindenkinek.

A módszer leírása:

A megvalósításhoz Mikrotik RouterBOARD 951G-2HnD-t használok, ami egy sokkal professzionálisabb eszköz, mint a hagyományos a lakosság által használt Access Pointok.

A router egyszerre csak egy DHCP[17] szervert képes futtatni, vagyis csak egy IP[18] tartományon tud IP címeket kiosztani, de több IP tartományt is képes kezelni, ezekre az IP tartományokra statikus IP címekkel lehet csatlakozni. A különböző IP tartományok között nincs adatforgalom.



23. kép: IP tartományok

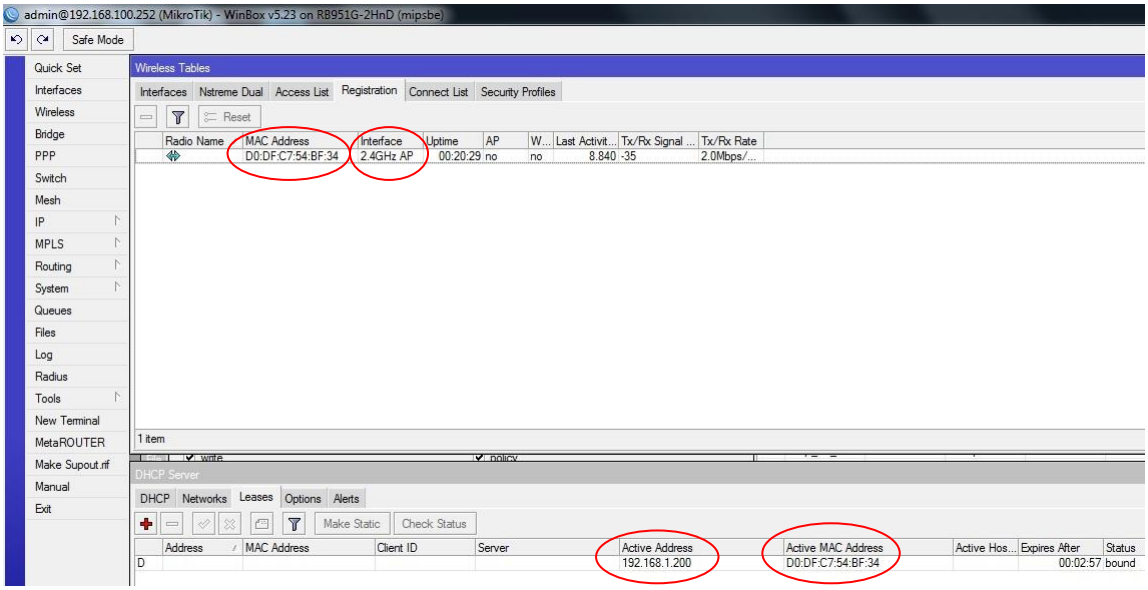
Forrás: Saját szerkesztés

A 24. képen látható, a két IP tartomány, a „KULSO TAMADO” és a „BELSO HALOZAT”. A „KULSO TAMADO” dinamikus IP-t használ, vagyis az Access Point ossza ki az IP címet a rá csatlakozó eszköznek, a 192.168.1.100-192.168.1.200-ig, vagyis a 192.168.1.X-es tartomány a hálózatot támadó eszközök tartománya. Ahhoz, hogy ez a tartomány egy honeypot legyen, nincs más dolgunk, csak rácsatlakoztatni egy szervert, és néhány munkaállomást (virtuális, vagy igazi), feltölteni őket „digitális

17 DHCP: Dynamic Host Configuration Protocol
18 IP: Internet Protocol

hulladékkal” (olyan fájlokkal, amik teljesen értéktelenek, de a támadó érdekesnek találja őket) és internetet rendelni az IP tartományhoz. Így a támadó csak annyit lát az egészből, hogy a WPA2 titkosítás feltörése után IP címet kapott, bent van a hálózaton, van internet kapcsolat, és lát néhány eszközt is, ez épp elég ahhoz, hogy a támadó el legyen foglalva egy darabig.

Az AP-t sem képes támadni a támadó, mert van rá lehetőség, és be is állítottam, hogy ebből a 192.168.1.X IP tartományból ne lehessen elérni a 80-as (böngészőn keresztül) és a 8291-es (winbox-on keresztül) portot az AP menüjét, így semmilyen beállítást nem módosíthat a támadó.

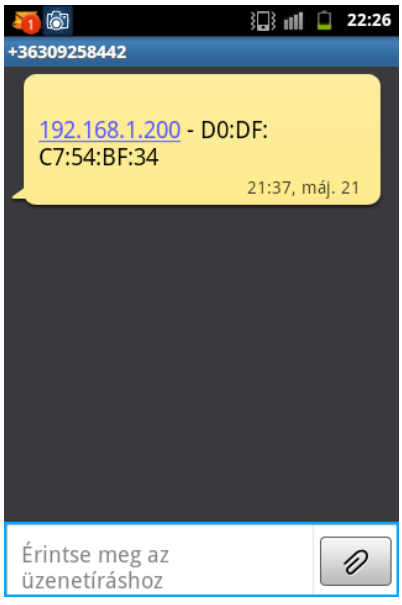


24. kép Támadó eszköz adatai

Forrás: Saját szerkesztés

A 24. képen látható, amint az AP kilistázza a támadó eszközök adatait, jelen esetben egyet. A képen látható, az eszköz MAC címe, IP címe, melyik interfacere csatlakozott…

A Mikrotik képes SMS-t küldeni a különböző eseményekről, így az is beállítható rajta, hogy értesítést küldjön arról, ha valaki rácsatlakozik a külső hálózatra. A 25.képen látható egy ilyen értesítés. A Mikrotik elküldte SMS-ben a támadó IP címét, és MAC címét. Az SMS küldéshez egy USB



25. kép: SMS értesítő

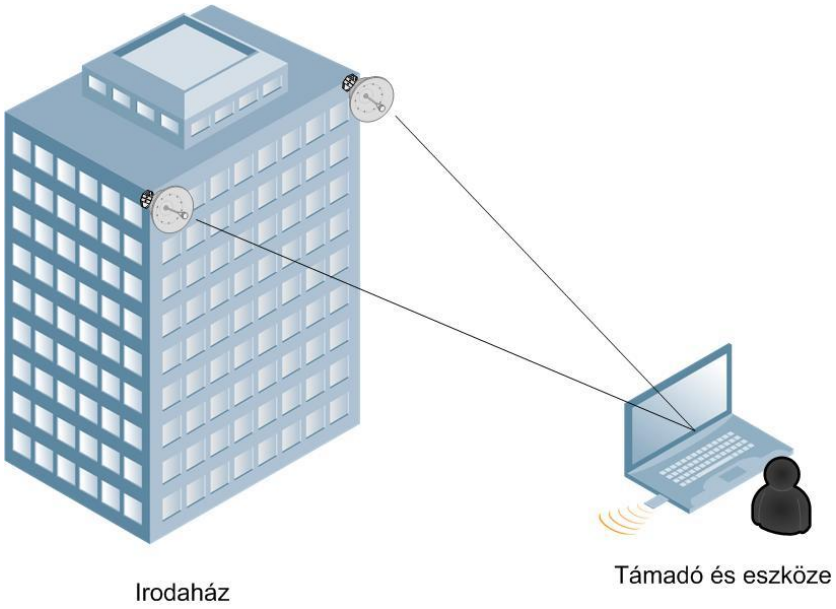
Forrás: Saját szerkesztés

stick is szükséges (Mobilnet), hiszen az SMS-t valamelyik mobilszolgáltató hálózatán keresztül fogja elküldeni.

A „BELSO HALOZAT”-ra való bejutáshoz statikusan kell felvenni a 192.168.100.100-192.168.100.102 IP címig valamelyiket (a példa szerint). Célszerű nem nagyobbra venni az IP tartományt, mint amekkorára szükség van.

5.3.3 Helymeghatározás kültéren

A támadás tényének realizálása után minél gyorsabban el kell kezdeni a támadó lokalizálását, hiszen a támadó nem marad örökre a hálózaton, így még az előtt ki kell érnie és intézkednie a beavatkozó erőknek, mielőtt a támadó kiszáll a hálózatról. A helymeghatározáshoz két módszert dolgoztam ki, az egyiket kültéren alkalmazom, a másikat pedig beltéren.



26. kép: Kültéri helymeghatározás vázlat
Forrás: Saját szerkesztés

Kültéren a támadó lokalizációját a terveim szerint irányított antennákkal, valósítom meg, a 26. képhez hasonlóan. A mérést végző számítógép megfelelő automatika használatával az irányított antennákat a legerősebb jelintenzitás irányába fordítja, és az antennák irányvonalának metszetében található a támadó. Az épület minden sarkára kell elhelyezni antennákat, ami egy téglatest alakú épület esetén 4 antennát jelent, ezek közül 2-3 antenna látja a támadót, az elhelyezkedésétől függően, de a helymeghatározáshoz 2 antenna elégséges.

Ennél a fajta helymeghatározásnál az ismert helyen (a térben minden koordinátája ismert) elhelyezett antennák horizontális és vertikális szögelfordulásait mérjük az épület síkjaihoz képest.

A helymeghatározás az alábbi számítások elvégzése után lehetséges:

Jelmagyarázat:

Mért értékek:

$m_é$= az épület magassága

sz= az épület szélessége

α= 1. antenna horizontális szögelfordulása

β= 2. antenna horizontális szögelfordulása

δ= 1. antenna vertikális szögelfordulása

ε= 2. antenna vertikális szögelfordulása

Számítandó adatok:

γ= 180°-α-β

z= segédváltozó

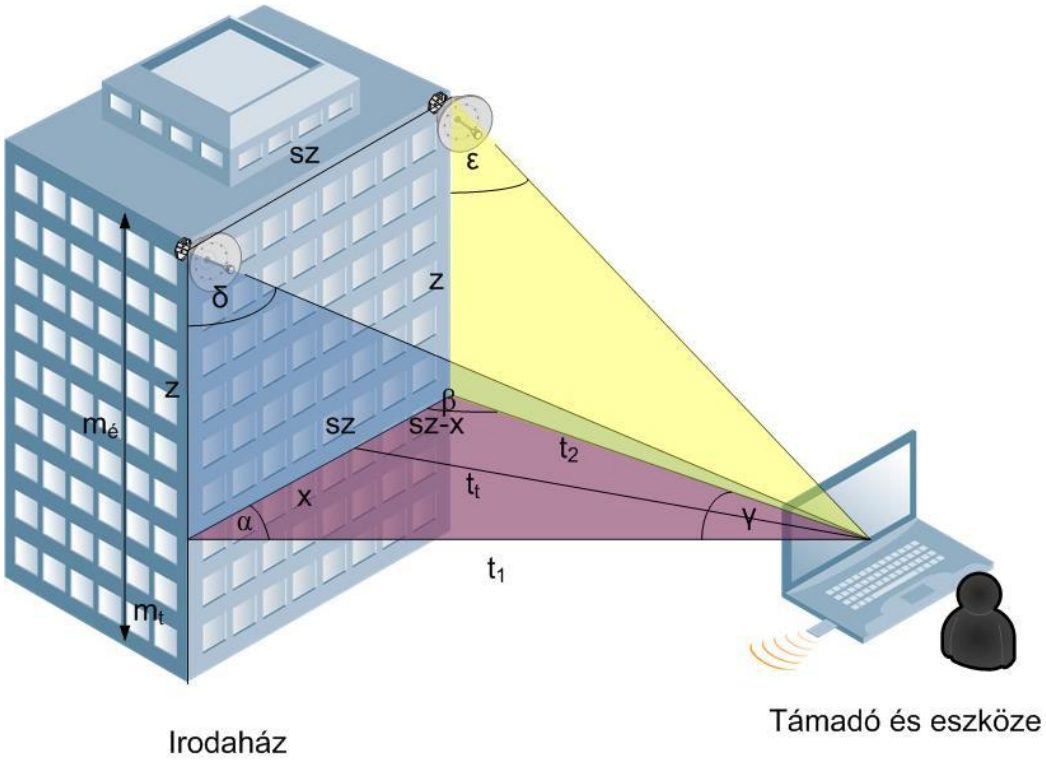
x= segédváltozó

m_t= a támadó magassága

t_t= a támadó épülethez viszonyított távolsága

t_1= segédváltozó

t_2= segédváltozó



27. kép Kültéri helymeghatározás szemléltető ábra

Forrás: Saját szerkesztés

A számításokhoz alapvetően 3 síkot kell meghatározni, az általam kékkel, pirossal, és sárgával jelölt síkokat. A kék és a sárga egy-egy derékszögű háromszög, a piros legvalószínűbb esetben általános, ritkább esetben egyenlő szárú vagy szabályos háromszög.

A számítás menete:

Piros sík:

$t_1=(sz*\sin\alpha)/\sin\gamma$

$t_2=(sz*\sin\beta)/\sin\gamma$

Egyenletrendszer:

I $x^2+t_t^2= t_1^2$ II $(sz-x)^2+t_t^2= t_2^2$ / I-II

$x^2 -(sz-x)^2= t_1^2- (t_2)^2 \rightarrow x= (t_1^2- (t_2)^2+sz^2)/(2*sz)$

$t_t^2 + x^2= t_1^2 \rightarrow t_t=\sqrt{(t_1^2- (x)^2)}$

Kék sík

$\text{tg}\,\delta=t_1/z \rightarrow z=t_1/\text{tg}\,\delta$

Sárga sík

$\text{tg}\,\varepsilon =t_2/z \rightarrow z=t_2/\text{tg}\,\varepsilon$

$m_t=m_é-z$

A t_t és az m_t a támadó épülethez viszonyított távolsága, ez a 2 adat, az x, és egy térkép kezelő program segítségével akár térképen is megjeleníthető a támadó pontos helye.

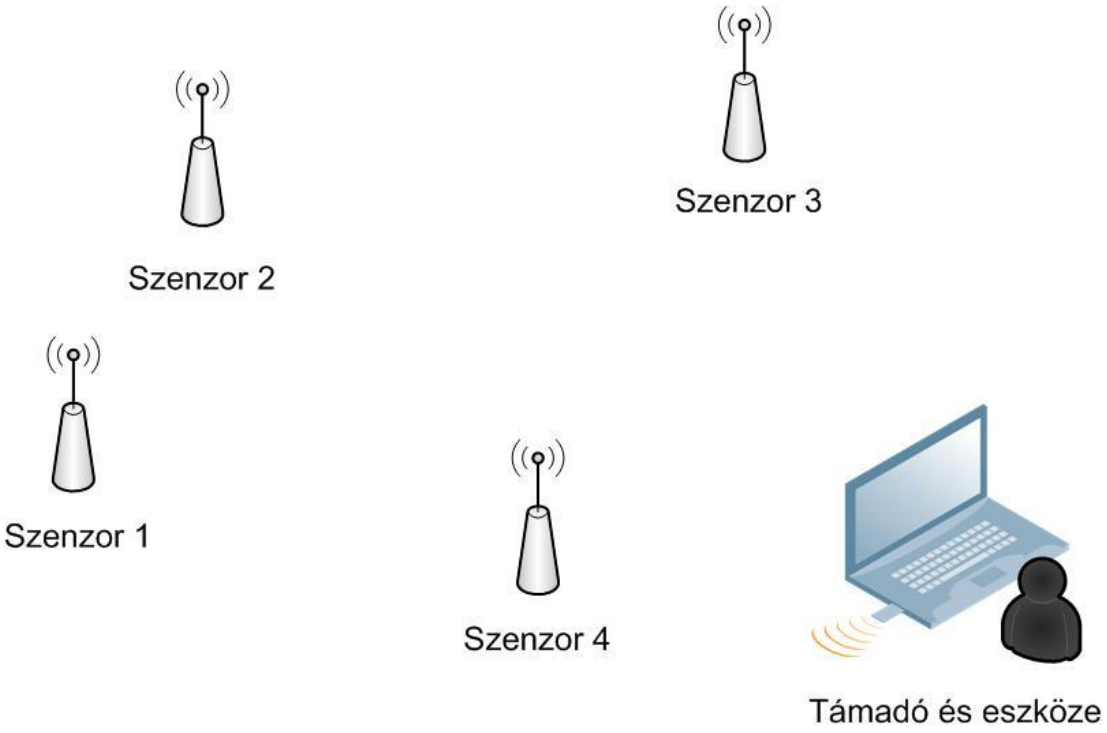
Annak érdekében, hogy a beavatkozó erőket további segítséggel lássuk el a támadó helyének megtalálásában, optikai felderítést is javaslok, amely közvetlen az antenna alá, vagy felé elhelyezett kamerát jelenti, vagyis, mivel kültéren alkalmazom ezt a lokalizációs formát az optikai rálátás majdnem minden esetben megvan.

A beavatkozó erők megkaphatják, azt az információt pl., hogy a parkolóban az egyik autóból törtek be a hálózatra, az autónak megadható a továbbiakban a rendszáma, színe, típusa.

5.3.4 Helymeghatározás beltéren

A beltéri helymeghatározást párhozamosan el kell indítani a kültérivel. Már léteznek megoldások WLAN eszközök helyének meghatározására, és mindegyik ezt a módszert alkalmazza, vagyis a kliens által sugárzott jel erősségét mérik. A legtöbb esetben a mérést valamilyen speciális szenzor végzi, amely az adatokat egy szerver gép fele továbbítja, ami az adatokat kiértékeli, és térképen megjeleníti.

A legnagyobb nehézség, effajta lokalizációnál, hogy minden mérést egyénileg ki kell értékelni, nem lehet már korábban kimért adatbázisra támaszkodni, mivel nem tudjuk, hogy milyen eszközt használ a támadó, annak mekkora az adóteljesítménye, így nem meghatározható, hogy X dBm Y m-t jelent, még optikai rálátás esetén sem.



28. kép: Beltéri helymeghatározás vázlat

Forrás: Saját szerkesztés

Azonban fontos az adatbázis elkészítése, minél több a mérés egy intelligens rendszer annál pontosabban képes megbecsülni a támadó helyét, hiszen a szenzorok helye nem változik, az antennáik megegyeznek, így a fogott jelek valamilyen arányosítása a kulcs.

Arra is van lehetőség, hogy az épület minden helyiségében elhelyezzünk szenzorokat, így könnyedén meghatározható, adóteljesítménytől függően, hogy melyik szenzorhoz

van legközelebb a támadó, nagyobb termek esetén (pl. csarnokok) azonban így is több eszközt kell elhelyezni a lehető legpontosabb mérés érdekében.

Ez a módszer kültéren is alkalmazható, bár személyes véleményem szerint kültéren az irányított antennás megoldás sokkal eredményesebb.

5.3.5 Jogi háttér

Köszönhetően annak, hogy a vezeték nélküli eszközök felderítése még szinte alig létező technológia mindössze néhány cég foglalkozik vele, és ők is elsősorban tárgyak nyomon követésére használják (pl. nagy értékű tárgyak nyomon követése).
A lokalizáció alapvető személyiségi jogokat sért, de mivel ebben az esetben vezeték nélküli hálózatot támadó személyről van szó:

2011. évi CXII. törvény
Az információs önrendelkezési jogról és az információszabadságról

„6. § (1) Személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése
b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.” [24]

A törvény ezen paragrafusa természetesen nem terjed ki olyan személyekre, akik nem minősülnek támadónak, de ez már nem tartozik a szakdolgozatomhoz.

A szakdolgozatom során már több alkalommal utaltam a „beavatkozó erő”-re, és egyetlen egyszer nem neveztem őket vagyonőrnek, vagy másnak.
Ennek oka, hogy jelen jogállás szerint a vagyonőr az általa őrzött objektum határain belül vagyonőr, azt elhagyva automatikusan civilnek minősül, és minden jogosultságát elveszíti:

2005. évi CXXXIII. törvény

A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

„26. § (1) A vagyonőr a megbízó közterületnek nem minősülő létesítményének őrzése során jogosult:

a) a területre belépő vagy az ott tartózkodó személyt kiléte igazolására, a belépés, illetőleg a tartózkodás céljának közlésére, jogosultságának igazolására felhívni, ennek megtagadása vagy a közölt adatok nyilvánvaló valótlansága esetén - a megbízó eltérő rendelkezésének hiányában - az érintett belépését, ott-tartózkodását megtiltani, és távozásra felszólítani;

b) a területre belépő vagy onnan kilépő személyt csomag, illetve menet-, szállítási okmány bemutatására felhívni;

c) a területen tartózkodó vagy onnan kilépő személyt - a 28. § rendelkezései szerint - csomagja tartalmának, járművének, valamint a szállítmánynak bemutatására felhívni;

d) a jogsértő személyt magatartása abbahagyására felhívni;

e) elektronikai vagyonvédelmi rendszert alkalmazni;

f) a területre belépők ellenőrzésére fegyver-, illetve robbanóanyag-kutató műszert alkalmazni és a közbiztonságra különösen veszélyes eszközök bevitelét megtiltani.” [25]

Jelen jogállás szerint az objektum területén kívül a rendőrség az egyetlen aki intézkedhet, nem szerencsés jogállás, de mivel ez nem egy olyan technológia, ami már régóta használt, és a köztudatban is él, így még nem alkottak hozzá megfelelő jogi környezetet.

ÖSSZEGZÉS

A biztonság az ember számára folyamatos, de el nem érhető igény. Az ember a biztonságnak csak bizonyos szintjeit képes elérni, legyen szó akár saját maga-, tárgyi-, vagy szellemi- értékeinek biztonságáról. Minél magasabb szintű biztonságra vágyik az ember annál nagyobb anyagi ráfordítást igényel.

Szakdolgozatom a vezeték nélküli hálózatok biztonsági kérdéseivel foglalkozik, megírásánál ezen hálózatok védelmi rendszeréhez próbál egy újabb eszközt hozzátenni.

Szakdolgozatom megírásánál célul tűztem ki magam elég, ismertetni a vezeték nélküli hálózatok eszközeit, az ide vonatkozó szabványokat, a vezeték nélküli hálózatok védelmének a módjait, azokat a támadási formákat, amikkel támadhatók ezek a hálózatok, ismertetni a rádióhullámokkal kommunikáló eszközök helymeghatározásának módszereit, és egy olyan módszer megtervezése, és kidolgozása, amellyel felderíthetőek a hálózat támadói.

Úgy vélem az első öt kritériumnak maradéktalanul megfeleltem, szakdolgozatom a lehető legaktuálisabb technológiákat figyelembe véve íródott.

A hatodik kritériumnak csak részben feleltem meg, ugyan is megtervezni sikerült megterveznem, egy olyan módszert, amellyel felderíthetőek egy vezeték nélküli hálózat támadói, a módszer gyakorlatba történő átöltetése azonban idő, erőforrás és programozási ismeretek hiányában csak részben megvalósítottak.

Sikerült egy olyan rendszer felállítása, amely kiszűri a gyengébb támadásokat, elkülöníti és egy olyan térbe száműzi azokat a támadókat, akiknek mégis sikerül áttörni a hálózat védelmét, megfelelő mennyiségű adattal látja el a támadót annak érdekében, hogy ne bontsa a kapcsolatot idő előtt, és két olyan módszer elveit fektettem le, amelyek alkalmasak az ilyen jellegű támadások támadóinak felderítéséhez.

A téma nagyságát, aktualitását figyelembe véve egy még számos új kutatás kell a téma kidolgozásához és megfelelő körbejárásához.

A szakdolgozatom remek kiindulási alap lesz akár saját magamnak, akár másnak további kutatásokhoz.

Köszönetnyilvánítás

Szeretnék köszönetet mondani Dr. Varga Péter Jánosnak, és Patkós Bélának, hogy segítségükkel, és tanácsaikkal segítették szakdolgozatom elkészültét.

IRODALOMJEGYZÉK

1. Bodnár Ádám: Rengeteg tabletet fognak eladni [Online] 2010. 10. 18. [Letöltve: 2013.05.06.] http://www.hwsw.hu/hirek/45477/tablet-piac-gartner-apple-ipad.html
2. Szőke Lajos: Vezeték nélküli hálózatok tervezése 2007 [Online] [Letöltve: 2012.09.22.] http://tiszai.tricon.hu/Szakdolgozat.pdf
3. wikipedia.org: IEEE 802.11 szabványcsalád [Online] http://hu.wikipedia.org/wiki/IEEE_802.11 [Letöltve: 2012.11.05.]
4. Kilbertus Viktor: Wireless AC1750 Cloud: D-Link router sebességmániásoknak [Online] 2012. 09. 28. [Letöltve: 2012.11.05.] http://infovilag.hu/hir-25133-wireless_ac1750_cloud_d_link_router_sebe.html
5. mobilix.hu: Asus router, [Online], http://www.mobilx.hu/images/detailed/asus_rt-n66u_router_00.jpg [Letöltve: 2013.04.09.]
6. forum.notebookreview.com: Asus laptop, [Online], http://forum.notebookreview.com/what-notebook-should-i-buy/260700-nice-asus-laptop-920-a.html [Letöltve: 2012.11.21.]
7. ipon.hu: Asus netbook, [Online], http://ipon.hu/_userfiles/Image/Gabriel/Minilaptopok/ASUS_N10_netbook_1-nagy.jpg [Letöltve: 2013.05.12.]
8. altair.ca: PC, [Online], http://altair.ca/wp-content/uploads/2011/06/Pc.jpg [Letöltve: 2013.03.06.]
9. urdesign.it: Sony Tablet, [Online], http://www.urdesign.it/wp-content/uploads/2013/02/1-sony-xperia-tablet-z.png [Letöltve: 2013.04.09.]
10. sonymobile.com: Okostelefon, [Online], http://www.sonymobile.com/global-en/products/phones/xperia-j/ [Letöltve: 2013.04.09.]
11. secron.hu: Netvadász készlet, [Online], http://www.secron.hu/vadasz.html [Letöltve: 2013. 03. 17.]
12. Dr. Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme 2007, [Online], [Letöltve:2013.03.27.], http://193.224.76.4/download/konyvtar/digitgy/phd/2008/muha_lajos.pdf

13. wikipedia.org: Trójai program, [Online] http://hu.wikipedia.org/wiki/Tr%C3%B3jai_program [Letöltve:2013.03.27.]
14. wikipedia.org: Hoax, [Online] http://hu.wikipedia.org/wiki/Hoax [Letöltve:2013.03.27.]
15. Varga Péter János: Kritikus információs infrastruktúrák vezeték nélküli hálózatának védelme, 2012 [Online] http://hhk.uni-nke.hu/downloads/tudomanyos_elet/kmdi/2012/Varga_Peter_Janos_phd_terveze te.pdf [Letöltve:2013.03.17.]
16. wardrivers.uw.hu: wardriving [Online] http://wardrivers.uw.hu/wardriving.html [Letöltve: 2013.04.15.]
17. wikipedia.org: wardriving [Online] http://hu.wikipedia.org/wiki/Wardriving [Letöltve: 2013.04.15.]
18. digistreet.hu: TP-LINK nano router, [Online] http://digistreet.hu/hirek/meretevel-hodit-a-tp-link-tl-wr702n-wireless-n-nano-router [Letöltve: 2013.04.15.]
19. firewalls.com Evil Twin [Online] http://www.firewalls.com/media/upload/image/wifi_phishing.PNG [Letöltve: 2013.04.18.]
20. huwico.hu: Hotspot paranoia [Online] http://www.huwico.hu/node/544 [Letöltve: 2013.04.18.]
21. veracode.com Man in the Middle [Online] http://www.veracode.com/images/mitm-flow.gif [Letöltve: 2013.04.18.]
22. fonepics.net: Access Denied, [Online] http://fonepics.net/uploads/pictures/big_images/access_denied.jpg [Letöltve: 2013.04.20.]
23. Magyari Béla: A rádiótechnika. könyvei 17 1956 http://www.ha5mrc.hu/library/terjedes/Florian_Endre_hullamterjedes.pdf [Letöltve: 2013.04.29.]
24. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [Online] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV [Letöltve: 2013.05.21.]

25. 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól [Online] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0500133.TV [Letöltve: 2013.05.21.]

MELLÉKLET:

1. melléklet