HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Illési Zsolt
illesi.zsolt@proteus.hu

Varga Péter
varga.peter@kvk.uni-obuda.hu

WARDRIVING ÉS A TÉRINFORMATIKA

Absztrakt

A technika fejlődésével nő a mobilitás iránti vágyunk. Ennek egyik lehetséges megvalósítása ha olyan munkahelyeket, szórakozó helyeket és lakhelyeket alakítunk ki, ahol mobil eszközeinkkel tudjuk végezni mindennapi tevékenységeinket. A rádiós hálózatok ilyen megoldást nyújtanak. A cikkben bemutatjuk a rádiós hálózatokra irányuló főbb támadási módszereket és a védekezés egyfajta megközelítését, amely maga a felderítés. Ennek a megelőző felderítési módszernek a főbb eszközei a wardriving és a térinformatika.

With technology development increases our desire toward mobility. One possible solution if we develop workplaces, pleasure-grounds, and homes where it is possible to deal with everyday routines with mobile devices. Radio networks provide appropriate solutions to mobility needs but also raise new vulnerabilities and threats. In this paper we summarize the main attack methods which are targeting radio networks, and we also present one possible way of defence, the Wi-Fi enumeration supported with geographic information application. The main tools for this preventive enumeration are wardriving and GIS.

Kulcsszavak: *AP, GPS, GIS, wardriving, Wi-Fi, térinformatika*

BEVEZETÉS

Az információs és kommunikációs technológia (ICT) fejlődése és egyre szélesebb térnyerése új technológiai trendet hozott hétköznapjainkba, mely középpontjában a mobilitás áll. Ezt úgy tudjuk elérni, ha informatikai rendszereinket vezeték nélküli hálózati szegmenssel látjuk el. Ez a trend egyre jobban megfigyelhető a vállalatoknál, infrastruktúra üzemeltetőknél és a magán szférában is. A komplex rendszerek elterjedésével nő az azokkal kapcsolatos támadások száma is. A támadók legtöbbször nem saját hálózatukat használják, hanem egy kiválasztott, általában gyengén védett hozzáférési ponthoz (Access Point, AP) csatlakoznak. Ezt azért tudják megtenni, mert felmérések szerint az AP-ok 60%-a nem rendelkezik megfelelő

biztonsági beállításokkal. A cikkben a vezeték nélküli hálózat (Wi-Fi) elleni támadások közül a wardriving és a térinformatika kapcsolatát mutatjuk be.

Célkitűzéseink között szerepel, hogy rámutassunk arra, hogyan fordíthatjuk a wardrivingot mint felderítési formát saját hálózatunk védelmére.

WLAN HÁLÓZATOK, FENYEGETÉSEK

A vezeték nélküli hálózat (Wi-Fi) egyik fő komponense a hozzáférési pont (Wireless Access Point, WAP) amely egy olyan kommunikációs eszközt jelent, amely mások számára elérhetővé teszi a Wi-Fi hálózat használatát, ezek rendszerint a Wi-Fi és a kábeles hálózatot összekötő útválasztók. A másik fő komponens a Wi-Fi berendezés, amely olyan eszköz, ami képes a Wi-Fi hálózaton keresztül kommunikálni. Wi-Fi hálózat létrejöhet hozzáférési pont(ok) között; hozzáférési pont és Wi-Fi berendezés(ek) között, és Wi-Fi berendezések között közvetlenül. [1]

A vezeték nélküli hálózatokat és állomásokat többféle támadás érhet. Ezen támadások közül a legnépszerűbbek külön nevet is kaptak.

Wardriving

A wardriving során a támadó célja, hogy behatoljon egy vezeték nélküli hálózatba és ott kihasználva a hálózat esetleges internet csatlakozását, ő maga ingyen internethez juthasson. Ehhez először keresni kell egy lehetőség szerint gyenge védelemmel ellátott Wi-Fi-t. Ezt általában egy gépkocsiban elhelyezett laptop segítségével teszi a támadó, és miután célt ért, leparkol és megkezdi a támadást. Innen ered az elnevezés.

Evil twin

Az evil twin a gonosz iker. A támadó célja, hogy megtévessze a felhasználókat és ők így az eredeti hozzáférési pont helyett a támadóhoz csatlakozzanak. A támadó ezért felveszi a megtámadott hozzáférési pont azonosítóját. A támadás során a támadó visszatereli az eredeti hálózatba a forgalmat, annak érdekében, hogy a felhasználó semmit se vegyen észre, azonban a forgalom-továbbítás során ellopja a felhasználó értékes adatait, amelyek segítségével a későbbiekben megszemélyesítheti a felhasználót.

Szolgálatmegtagadás

Ennek a támadástípusnak a célja egy adott hozzáférési pont megbénítása. Ez történhet a fizikai rétegen keresztül zavarással (jamming), de akár magasabb rétegeket is kihasználhat a támadó.

Lehallgatás

A lehallgatás során a támadó belehallgat a hálózatba és próbál mások kommunikációjából értékes adatokat szerezni.

Az itt felsorolt támadási formák közül a wardriving alkalmazható saját hálózatunk biztonságosabbá tételéhez.

A VÉDEKEZÉS

Ahhoz, hogy meg tudjuk védeni saját hálózatunkat tisztában kell lennünk a körülöttünk levő hálózati elemek csoportjaival. A beazonosítás legegyszerűbb módja a felderítés. A Wi-Fi hálózatok technikai felderítése során szerzett adathalmaz azonban önmagában nem vagy csak nehezen értelmezhető. A vizsgálat kulcsfontosságú eleme egy GIS (Geographic Information System) vagy térinformatikai alkalmazás, amely lehetővé teszi az összegyűjtött információknak feldolgozását és térbeli megjelenítését. A megjelenített információk alapján elkülöníthetjük a hálózatunkra veszélyt jelentő külső hálózati elemeket melyek hatósugara a saját hálózatunkig elér.

WARDRIVING MINT A FELDERÍTÉS EGYIK ESZKÖZE

Ez a típusú tevékenység speciális hardver és szoftver környezetet kíván. Hardver oldalról a következő eszközöket kell használni:

- Autó – ez a tipikus wardriving (vagy bicikli – ebben az esetben a warbiking-ról beszélhetünk).
- Hordozható számítógép, ami lehet laptop, kéziszámítógép vagy okostelefon, melyben van, vagy csatlakoztatható, a csomagok lehallgatásához szükséges „monitor” módba kapcsolható WLAN hálózati kártya.
- WLAN antenna. Erre akkor van szükség, ha nem elégszünk meg az eszközbe épített antenna vételi paramétereivel.
- Globális Helymeghatározó készülék (GPS). A pontos helymeghatározáshoz elengedhetetlen.

A következő képen egy átlagos hardveres összeállítást látható (1. ábra).

1.ábra: A wardriving elengedhetetlen eszközei [2]

A wardriving szoftveres oldalát két csoportra lehet bontani

- a felderítésért felelős,
- a kiértékelésért, megjelenítésért felelős programok.

A vezeték nélküli hálózatok felderítéséhez használt programokat platform szerint szokták megkülönböztetni. Linux-os operációs rendszerekhez a következő programokat használják:

- Airsnort: adatfolyamot analizál,
- Airtraf: hálózati protokoll szkenner,
- Kismet: adatfolyamot analizál.

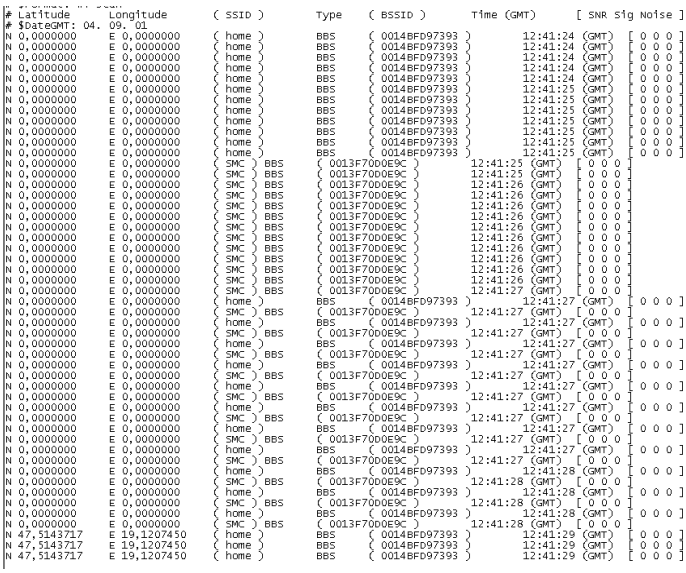
Microsoft windows-os rendszerekben a következő programokat használják:

- Inssider: adatfolyamot analizál, megmutatja és tárolja a már megtalált hálózati elemeket.
- Aerosol: adatfolyamot analizál.

Kéziszámítógépes környezetben a következő programokat használják:

- Ministubler: adatfolyamot analizál, megmutatja és tárolja a már megtalált hálózati elemeket
- Wifiofum: adatfolyamot analizál, megmutatja és tárolja a már megtalált hálózati elemeket.

A kiértékelés és a megjelenítés a felderítő programok lementett napló fájljaiból történik. Ha a hardverhez GPS vevőt csatlakoztattunk később nem csak a hálózati eszközökre vonatkozó információkat elemezhetjük hanem a lementett koordináták segítségével térképre is illeszthetjük a gyűjtött adatokat. A következő ábra egy ilyen adathalmaz részt mutat (2. ábra):



2.ábra: Egy wardriving során lementett adatok egy része (saját szerkesztés)

A mért adatok vizualizálását a térinformatikai szoftverek teszik lehetővé.

A TÉRINFORMATIKA

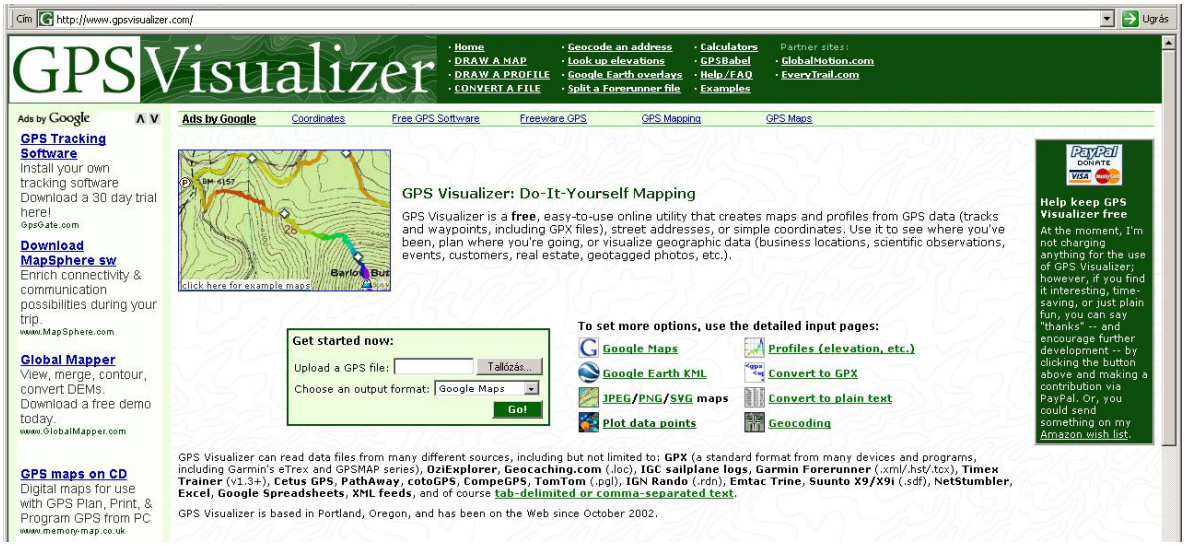
Térinformatika, geoinformatika a digitális térképekre épülő informatika, olyan interdiszciplináris terület, amely elsősorban földrajzi, térképészeti és informatikai szakismeretekre épül.

Térinformatikai rendszerek (térinformációs rendszer) alatt térképi alapú információs rendszert értünk, amely grafikus (térképi) és nem grafikus (leíró) adatokat együtt, integráltan tud kezelni.

A GIS (Geographical Information System) olyan földrajzi információs rendszer, amely tágabb értelemben térképi alapú információs rendszer, szűkebb értelemben csak a kimondottan földrajzi adatokra épülő (pl. környezetvédelmi) rendszereket jelenti, és nem tartalmazza pl. a közműnyilvántartást.[3]

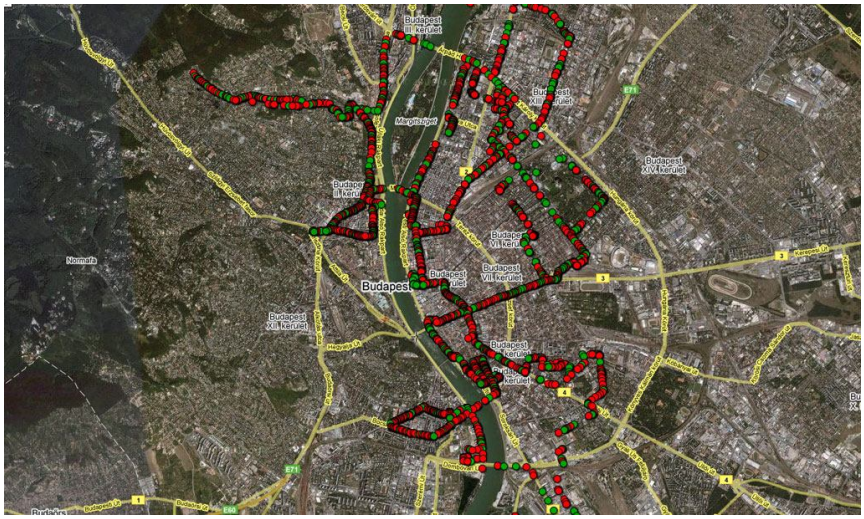
A térinformatikai rendszerek manapság bárki számára elérhetőek. Több alkalmazás is megtalálható az interneten, amely lehetővé teszi megfelelő konverziók után saját mérési pontjaink megjelenítését valamilyen térinformatikai programban.

Digitális térképeken úgy lehet megjeleníteni a vizsgálati eredményeket, hogy a mentett információkat a térinformatikai rendszer számára átkonvertáljuk. A konverziót el lehet végezni segédprogramokkal, de a legegyszerűbb, ha egy erre a feladatra készített weboldalt használunk. A következő képen egy ilyen portál látható (3. ábra):



3.ábra: A GPS naplók konvertálása [4]

A konverzió során elveszhetnek információk (például dátum, jelerősség, csatornaszám). Ezért célszerű több típust is kipróbálni ahhoz, hogy a kiértékelés és a megjelenítés minél teljesebb legyen. A megjelenítést többféleképpen végezhetjük el. Léteznek speciális webes alkalmazások erre a célra, de ezek az információ egy részének megjelenítésére alkalmasak. Ilyen portál például a maps.google.com. A konvertált napló fájl alapján a pontokat a térképre tudja illeszteni, de ezen kívül már csak a színekkel és piktogramokkal tud variálni. Ezt mutatja be a 4. ábra.



4.ábra: Budapest egy részének WLAN térképe [5]

A térképen a zöld pontok a nyitott hálózatokat jelzik. A felderített AP-ok koordinátáit a rendelkezésünkre álló adatok és GIS alkalmazások az út nyomvonalára illesztették, így a térkép közelítő pontossággal jelöli azok helyét.

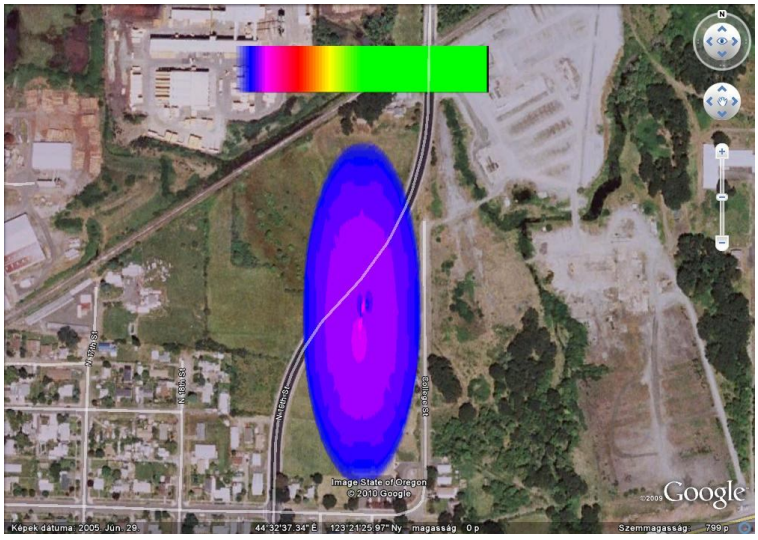
A VIZUALIZÁLÁS ÚJ MÓDSZERE

A vizualizáció abban tér el az előző pontban említettől, hogy egy speciális, erre a célra kifejlesztett PERL alkalmazást kell futtatnunk. A Footprint program a mért értékeinket MAC cím szerint leválogatva tudja értelmezni. Kiválasztva egy AP-ot leválogatja a hozzá tartozó mérési pontokat és generál hozzá két kép fájlt. Az egyik tartalmazza a mérésünk útvonalát, a másik a kiválasztott AP-unk rádiós hőtérképét. [6] A rádiós hőtérképet a táblázatban megjelölt jelszintekhez tartozó színekkel generálja le az alkalmazás.

Jelszint (dB-ben)	Színek
-100dB < Jelszint < -95dB	átlátszó -> kék
-95dB < Jelszint < -90dB	kék -> lila
-90dB < Jelszint < -80dB	lila -> piros
-80dB < Jelszint < -70dB	piros -> sárga
-70dB < Jelszint < -60dB	sárga -> zöld
-70dB < RSSI < -20dB	zöld

A mért jelszintekhez deklarált színek a hőtérképen (saját szerkesztés)

A végső megjelenítéshez a Google Earth programot használunk. A két generált kép és a Footprint által generált koordináták megadásával a Google Earth a helyére illeszti a képeket, és így majdnem pontosan azonosítható az AP helye és a Wi-Fi hálózat térerőssége (5.ábra).



5.ábra: Felderített AP-ok alakulása [7]

ELEMZÉS

A térképen megjelenített adatok alapján vizuálisan beazonosítható a saját és a minket körülvevő AP-ok lefedettsége. A méréseket úgy tudjuk teljes körűen elemezni, ha minden felderített AP-ra elvégezzük az elemzést, és a mért értékeket egy felületen külön rétegekben jelenítjük meg. Abban az esetben, ha a védeni kívánt infrastruktúra körvonalait rávetítjük az így kapott térképre, pontosan meg tudjuk állapítani a számunkra esetlegesen veszélyt jelentő Wi-Fi eszközöket. Ennek birtokában konfigurálhatjuk be rádiós hálózati elemeinket.

ÖSSZEFOGLALÓ

A Footprint alkalmazás segítséget nyújt az infrastruktúra üzemeltetőknek feltérképezni saját és környezetük rádiós térképét. A népszerű mondás szerint a rádióhullámok nem állnak meg a falak mentén, így jó esetben a felfedett AP-okat tiltani tudjuk saját rádiós eszközeinkben. Ezzel el tudjuk érni, hogy közvetlen környezetünkből ne érjen támadás.

A jövőben hogy hatékonyabbá lehessen tenni a Footprint alkalmazást autómatizálni szeretném, hogy ne csak egy AP-t vizsgáljon egyszerre, hanem az összes mért értéket helyezze a térképre. A védekezés az elsődleges, mert a védetlen vagy sebezhető végpontok egy támadás kiindulópontjaként szolgálhatnak, anonimitást biztosítanak a számítógép-hálózatokat jogellenesen használóknak, így a Wi-Fi AP-ok elleni támadások hatása szélsőséges esetben akár az egész nemzetbiztonságra is kihathat.

Felhasznált irodalom

[1] Illési Zsolt: *Wi-Fi hálózatok igazságügyi szakértői elemzése:Wi-Fi hálózatok felderítése,* Hadmérnök IV. Évfolyam 3. szám - 2009. szeptember pp. 285-302

[2] A wardriving elengedhetetlen eszközei
http://www.wardrive.net/wardriving/tools/ (2010.06.12)

[3] Dr. Katona Endre: *Térinformatika*, Jegyzet - Szegedi Tudományegyetem, 2009 p. 5
http://www.inf.u-szeged.hu/oktatas/jegyzetek/KatonaEndre/gis.pdf (2010.06.12)

[4] A GPS naplók konvertálása
http://www.gpsvisualizer.com/(2010.06.12)

[5] Budapest egy részének WLAN térképe
http://www.origo.hu/techbazis/internet/20070601utcannenetezz.html (2010.06.12)

[6] Connelly K., Liu Y., Bulwinkle D., Miller A., and Bobbitt I.: A Toolkit for Automatically Constructing Outdoor Radio Maps
http://www.cs.indiana.edu/surg/Publications/itcc2005_toolkit.pdf (2010.06.12)

[7] Felderített AP-ok alakulása
http://www.cs.indiana.edu/surg/Publications/itcc2005_toolkit.pdf

(2010.06.12)